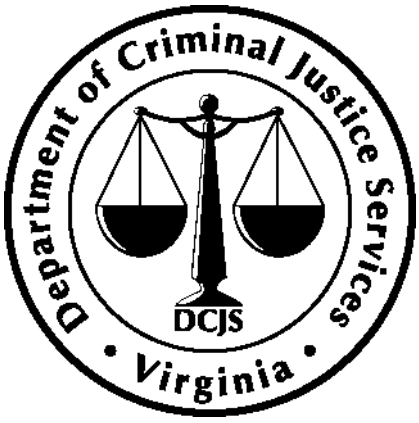

Business Case for Virginia Integrated Justice

Integrated Criminal Justice Information System

March 14, 2001

Table of Contents

Table of Contents (continued)

List of Figures

ICJIS Business Case

1. Introduction: Purpose and Scope

This document describes the Commonwealth of Virginia's Integrated Criminal Justice Information System (ICJIS) program, an initiative of the Secretary of Public Safety and the Virginia Department of Criminal Justice Services (DCJS). The ICJIS program is a response to the growing need to obtain greater efficiencies in the criminal justice system through improved inter-agency cooperation and information sharing.

After analyzing relevant business problems, the ICJIS Steering Committee and DCJS has concluded that the most cost-effective solution lies not in development of a totally new and massive system, but in the incremental upgrading and integration of existing information system assets. This Business Case describes the key challenges facing the Virginia criminal justice community in the area of integrated information management, and how these challenges may be addressed through improved business processes, enhanced technical capabilities, and adoption of inter-agency technical and data standards.

The Virginia ICJIS Business Case document presents a comprehensive explanation of the ICJIS program with each Section introduced by an Overview to provide focus on key points.

The document is organized as follows:

- Section 2 presents historical background and a vision for the benefits to be achieved through ICJIS implementation.
- Section 3 presents a summary of a detailed business problem analysis performed by DCJS.
- Section 4 presents a functional concept of operations for an integrated approach to criminal justice system information management.
- Section 5 discusses high-level functional system architecture requirements and trade-offs.
- Section 6 presents a high-level plan for ICJIS implementation.
- Section 7 is a brief closing summary and a list of the points of contact and Steering Committee representatives.

A separate standalone Executive Summary of the Business Case is also available from the ICJIS program office.

The material in this Business Case was developed through the cooperative effort of the ICJIS unit staff within DCJS and members of the ICJIS Steering Committee.

The ICJIS Steering Committee is comprised of representatives from stakeholder criminal justice organizations. They include:

- Department of State Police
- Department of Juvenile Justice
- Supreme Court of Virginia
- Department of Corrections
- Department of Motor Vehicles
- State Compensation Board
- Department of Information Technology
- Department of Technology Planning
- Chesterfield County (representing county governments)
- Department of Criminal Justice Services

Major technical consulting and editorial support to production of this document was provided by Litton PRC, under contract to DCJS.

The ICJIS Steering Committee, DCJS, and Litton PRC wish to thank the many criminal justice agency staff personnel who participated in interviews and surveys as part of the information gathering process. Without their professional insights and cooperation, this document would not have been possible.

2. Background and Need

Section Overview

Purpose: To describe the problems being addressed by ICJIS, and to describe how the program is structured to address those problems.

Key Points:

- The Virginia criminal justice community is very large and diverse, crossing many organizational and geographic boundaries, with complex and overlapping information requirements.
- Due to natural historical forces, current business practices and information systems place limits on the degree to which information—the lifeblood of any community—can be shared in an efficient, timely and integrated manner.
- The ICJIS program proposes community-wide adoption of an integration approach based on the SEARCH/NASIRE model—a cooperative model specifically designed for integration of autonomous systems maintained by independent agencies.
- The ICJIS program is designed to achieve cooperative implementation of this model via a combination of program management, policy analysis, standards development, data quality improvement, and system engineering activities. The ICJIS unit within DCJS is advised by a Steering Committee of representatives from key stakeholder agencies.
- Upon implementation, the ICJIS will provide major tangible operational benefits to criminal justice professionals statewide, and therefore improve public safety, confidence, and satisfaction with Commonwealth criminal justice services.

2.1 Problem Statement

The Virginia criminal justice community includes many government disciplines and crosses many organizational boundaries. As shown in Figure 2.2-1, the criminal justice mission encompasses a long chain of events and activities, beginning with investigation of a crime or complaint, through arrest and charging of a suspect, prosecution of the defendant, sentencing upon conviction, and incarceration, probation, or other monitored forms of corrections.

At each stage of the process, different combinations of state and local agencies are involved. Each agency collects and stores valuable information regarding the case and the individuals involved. Naturally, much of the information gathered by any one agency is of interest to all the other agencies involved in a case. In addition, agencies require current information about other agencies' activities and decisions affecting a case.

Historically, much of this information was originally recorded in non-digital form—

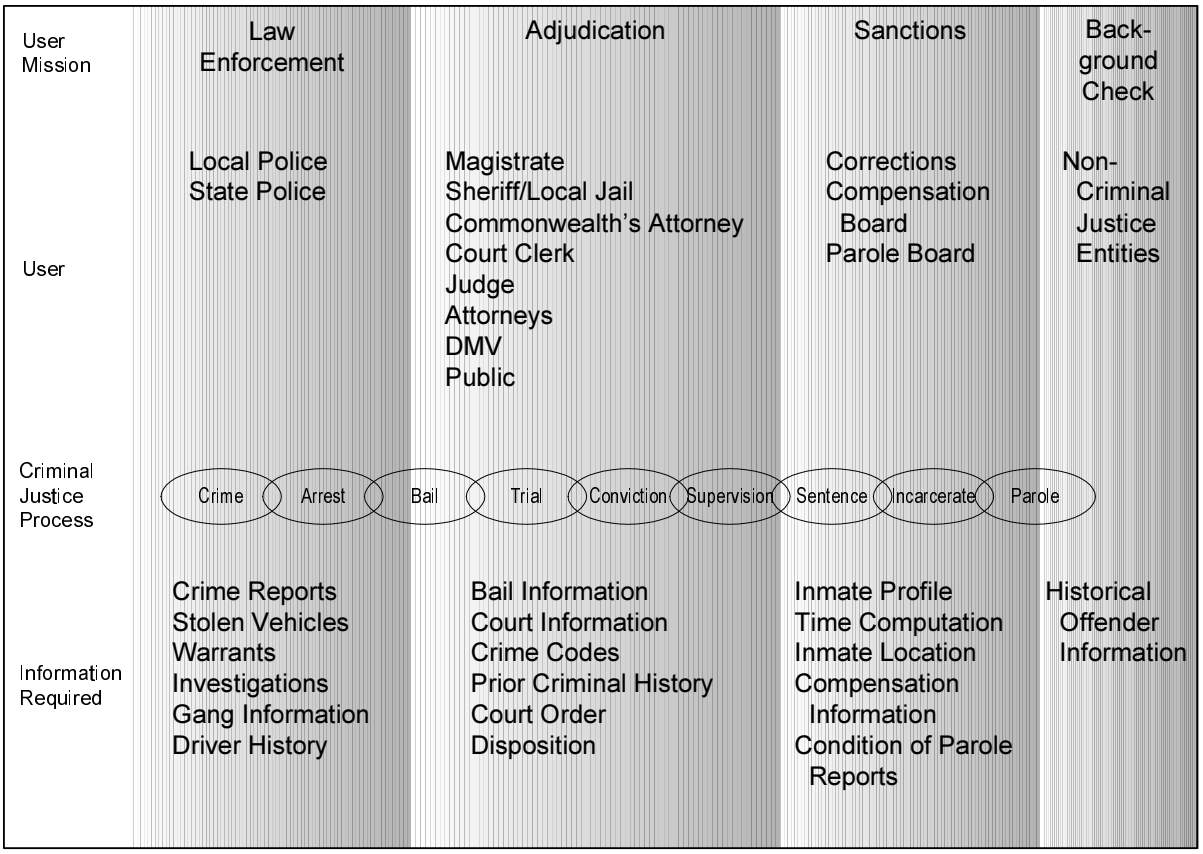

Figure 2.2-1. The Virginia criminal justice system encompasses a long chain of organizations, activities, and information requirements

e.g., handwritten or typed reports and forms, photographs, fingerprint cards, audio and video tapes. Over the years, computer-based information systems have been developed to manage more and more of this information in digital form. However, these systems have generally been designed to support one particular function within one particular agency. Such information systems are referred to as "stovepipe" systems, because they funnel a narrow range of data vertically back and forth between a function-specific database and a narrow range of users.

As a result of this legacy, the criminal justice community today is supported by a large number of independently developed information systems that have some stovepipe characteristics. These systems do a generally good job of supporting the functions and users they were designed to support (although some improvements may be needed). But the systems do not, and often cannot, always share the information they have with users and systems at other agencies that would benefit from access to the data.

The end result is that many criminal justice workers are forced to perform their missions and make decisions without benefit of all the information potentially useful to them. Alternatively, they are forced to delay their actions until they can gather the information using non-digital methods (e.g., by exchanging hardcopy documents, or communicating via telephone, fax, or e-mail). Often, there are no methods for promptly learning of a relevant event occurring at another agency except through person-to-person contact.

In addition, agencies often independently capture the same information, causing redundant effort and opportunities for errors and inconsistencies. In some cases, users at one agency are not even aware of the existence of data they need in other agencies' databases. Even when two agencies are aware of the existence of related data, they may not be able to easily share it, due to incompatibilities in agency computer systems, database formats, and/or retrieval keys.

The agencies themselves have taken positive steps to address these problems and shortcomings. Over the years, most agencies have vastly improved the level of integration within their own organizations, and many have cooperated to establish automated interfaces between organizations. While such initiatives have been very beneficial, the time has come to consider a strategic enterprise-wide solution. Without a unifying "big picture" view of the problems (and solutions), there can be little assurance that independent piecemeal solutions will ultimately tie together cost-effectively.

Another reason to take a strategic approach is the growing movement to integrate state systems with regional, federal, and even international criminal justice systems and networks. The problems discussed above are of course not unique to Virginia or to the criminal justice community. The same historical forces that led to development of stovepipe systems here caused similar results elsewhere. There are in fact many ongoing initiatives to achieve greater

A report on the Central Criminal Records Exchange, dated January 15, 2001, (http://www.apa.state.va.us/reports/special/searchreportname.asp) by the Auditor of Public Accounts, makes a number of comments and recommendations regarding the need for more complete integration of criminal justice systems.

"The development of a common data dictionary and data elements for all criminal justice computer systems and databases would allow for common reporting, exchanging, and sharing of information. Also, an environment of integrated information management will best accomplish data sharing."

"The lack of an integrated criminal justice system reduces the timeliness and accuracy of pertinent information. It also can pose a threat to public safety and individual civil rights."

"An integrated criminal justice system should support interoperable, portable, and scalable applications through data standards and formats, interfaces, and protocols. The systems must address data quality and integrity maintenance while providing users value-added functionality."

"Recommendation: Criminal justice information systems should adhere to information system development and data exchange standards to ensure accurate and timely sharing of information among systems."

integration of information, and interoperability of systems, at every branch and level of government.

As just one example relevant to the criminal justice community, there is at the federal level an initiative called the Global Justice Information Network (GJIN). Under the leadership of the U.S. Attorney General, this initiative is in the early stages of defining requirements for infrastructure standards capable of supporting cooperative sharing of information at all levels of the criminal justice community.

Clearly, what is needed is an approach that facilitates more integrated management of information among Virginia criminal justice agencies, while at the same time ensuring compatibility with emerging standards (such as those being defined by GJIN) for information sharing with the wider criminal justice community. ICJIS is Virginia's response to these requirements.

2.2 The Integrated Justice Vision

The Integrated Criminal Justice Information System (ICJIS) is an initiative of the Department of Criminal Justice Services (DCJS), one of 12 agencies within Virginia's Secretariat of Public Safety. The DCJS is charged with planning and carrying out programs and initiatives to improve the functioning and effectiveness of the criminal justice system as a whole. (§9-170 of the Code of Virginia)

The mission of the DCJS is to provide operational and support services to promote and enhance public safety in the Commonwealth through education, standards, forensic laboratory services, grant funding, information, programs, and technical assistance. In addition to providing a variety of direct services, the Department distributes federal and state funding to localities, state agencies, and nonprofit organizations in the areas of law enforcement, prosecution, crime and delinquency prevention, juvenile justice, victims services, corrections, and information systems.

DCJS is unique in state government because of its system-wide perspective on criminal justice. While it directs programs and services to each component of the system, it has an overarching responsibility to view the system as a whole, to understand how changes in one part of criminal justice will affect other parts, and to work to assure that plans and programs are comprehensive.

DCJS initiated the ICJIS program to facilitate dramatic and comprehensive improvements in the management of information in an integrated manner among the many Virginia criminal justice agencies and jurisdictions. Through ICJIS, DCJS seeks to promote an enterprise view of information as a shared strategic resource, without in any way compromising the data management and protection responsibilities of each agency.

The ICJIS program office is driven by the following vision statement:

> *The primary objective of integration is to improve criminal justice processing and decision-making through the elimination of duplicate data entry, access to information that is not otherwise available, and the timely sharing of critical data.*

In order to achieve this vision, the ICJIS program first set out to clearly define what is meant by integration, and to do so in a manner consistent with parallel initiatives in other states and at the national level.

After reviewing the state of the art, ICJIS has adopted a functional model for effective inter-agency integration proposed in a

SEARCH report, "Integration in the Context of Justice Information Systems: A Common Understanding," dated April 2000. SEARCH is The National Consortium for Justice Information and Statistics. Their report is available for downloading from www.search.org.

This model has been formally endorsed by the National Association of State Information Resource Executives (NASIRE), which proposed a similar approach in a report titled "Toward National Sharing of Government Information," February 2000, available at www.nasire.org. NASIRE is an association of chief information officers from all the states. Virginia is represented in NASIRE by the Secretary of Technology, Donald W. Upson.

Under the SEARCH/NASIRE model, there are five fundamental capabilities required to achieve true integration of multi-agency data resources:

- Allow authorized users at each agency to *query* local, regional, statewide and national databases for all relevant information about a person or case. An example might be to allow a local police investigator to determine whether a suspect has a criminal history at the state or national level.
- Allow one agency to *push* useful information to another agency, based on actions taken within the originating agency. An example might be to allow the state or local police to forward case data to the appropriate Commonwealth Attorney's office upon arrest and booking of a suspect.
- Allow a system to *pull* needed information from systems at other agencies for incorporation into the recipient agency's systems. An example might be to allow a police booking application to automatically retrieve information from a magistrate arrest warrant database to avoid having to re-enter some information redundantly.
- Allow a user at one agency to *subscribe* to a notification service that will automatically *notify* the recipient of events of interest elsewhere in the criminal justice system. An example might be to allow probation officers to request immediate electronic notification should any of their clients be arrested.
- Allow an agency to *publish* information regarding cases, events, and agency actions that may be of interest to other agencies. An example might be to post (perhaps on a web site) court schedules updated daily.

DCJS has added one more fundamental integrating capability to the basic model:

- *Assemble* data necessary for aggregate statistical analysis required for policy analysis, program evaluations, or research. An example might be to perform statistical analyses of recidivism rates correlated to criminal histories and types of correctional programs.

The underlying concept behind the SEARCH/NASIRE model is that information integration should mean much more than the simple sharing of data between agencies. Instead, integration should be viewed as a set of information processes that facilitate greater coordination of agency activities in performance of the overall criminal justice mission. The functions identified as *query*, *push*, *pull*, *subscribe*, *notify*, and *publish* (plus *assemble*) are needed to respond to different types of events and agency relationships. Together, these functions can be used to fundamentally improve criminal justice business processes.

The specific application of this model to the ICJIS environment will be detailed in Sections 3, 4, and 5 of this document.

2.3 ICJIS Program Concept

To achieve the integrated justice vision, the ICJIS program is pursuing a multi-pronged response to the integration problem. Just as the problem has many dimensions, so does the solution.

The ICJIS program sees its mission as being to achieve integration objectives through a variety of means as appropriate, including but not limited to: program management, policy analysis, standards development, data quality improvement, and system engineering. Each of these program components is described below.

2.3.1 Program Management

Understanding the information problems of integrated justice, as well as their solutions, requires an enterprise-level view of how information is used across the many independent agencies and jurisdictions in the criminal justice community. Organizationally, a central focal point is needed to reconcile the interests, and coordinate the efforts, of the many stakeholder organizations.

DCJS created the ICJIS program to serve as that focal point. The ICJIS serves as a program management structure for planning, facilitating, and coordinating the enterprise-wide integration effort. The key responsibilities of the program management component include:

- Promoting and facilitating an enterprise-wide view of criminal justice information as a strategic resource, across agency and jurisdictional boundaries.
- Identifying, planning, coordinating, and managing decisions, policies, and activities required to cost-effectively achieve the integrated justice vision.
- Acquiring, managing, and disbursing funds and other resources for this purpose.

When changes to state and local systems and processes are needed to achieve larger integration objectives, the ICJIS program's preferred method of operation is to develop standards and requirements through a cooperative effort involving the affected agencies, then issuing grants to agencies to design and implement the required changes.

To ensure that agency interests are properly represented in major decisions made by the ICJIS program, the program is advised by an inter-agency ICJIS Steering Committee. The membership includes representatives from key agencies expected to be most immediately affected by ICJIS implementation, either as key providers of ICJIS data, or as key users, or both. They include:

- Department of Corrections, which maintains records on state correctional facility inmates, as well as participants in other correctional programs.
- Department of Juvenile Justice, which maintains case and history records on state juvenile offenders and their families. Sharing of this data must be carefully managed, as much of it is restricted by law.
- Department of Motor Vehicles, which maintains a large database of state drivers, including relatively recent photographs.

- State Compensation Board, which maintains jail commitment and release data to support state revenue allocations to local jurisdictions.
- Supreme Court of Virginia, which is the management agent for the entire state judicial system, including the Court of Appeals, Circuit Courts, General District Courts, Juvenile and Domestic Relations District Courts, and the local Magistrates.
- Virginia State Police, which maintains extensive databases on wanted persons, sex offenders, and criminal histories. The VSP also maintains state fingerprint files, and provides fingerprint matching services for state and local law enforcement agencies.
- Department of Information Technology, which provides major information technology services to Virginia state and local governments.
- Department of Technology Planning, which serves as the technology planning and policy development arm of the Secretary of Technology.
- Chesterfield County Information Systems Technology office, which provides representation for the requirements and concerns of local governments.
- Department of Criminal Justice Services, which manages the ICJIS project.

A current roster of Steering Committee members is given in Appendix A. The ICJIS Steering Committee meets on a regular basis to provide guidance on major decisions. It will be asked to help finalize and approve ICJIS plans and standards for achieving system integration objectives.

2.3.2 Policy Analysis

DCJS has embarked on the ICJIS program in the context of far-reaching information technology policy initiatives put into motion by Governor James Gilmore and supported by the Virginia General Assembly. Both the executive and legislative branches have voiced strong support for policies aimed at keeping Virginia in the forefront of application of advanced technologies to the delivery of critical services to the citizens of the Commonwealth.

Governor Gilmore created the nation's first office of a Secretary of Technology by Executive Order in May of 1998, appointing Donald W. Upson to the position. The office was subsequently established in statute by the General Assembly in 1999. The Secretary of Technology is now a Cabinet-level post reporting directly to the Governor with statutory responsibilities as Virginia's Chief Information Officer.

In August 1998, Governor Gilmore announced the creation of the Council on Technology Services (COTS), chaired by the Secretary of Technology, to develop a blueprint for state government information technology planning and decision-making. The Council membership includes representatives from state agencies, institutions of higher education, and local governments. Among other duties, COTS is charged with promoting the development of statewide standards, where appropriate, in all facets of Information Technology.

To support these statewide policies and initiatives, ICJIS will serve as a mechanism for coordinating an enterprise-wide view of the operational implications of information management policies and issues on the criminal justice community. The key

responsibilities of the policy analysis component include:

- Developing and maintaining an enterprise-wide model of information flows and interfaces across agency and jurisdictional lines.
- Providing recommendations and advice to decision-makers on information policy issues.
- Recommending changes to existing laws, policies, and procedures that have significant impacts on the ability of the criminal justice community to share useful information.

2.3.3 Standards Development

Agreement on standards—for processes, for data, for interfaces and infrastructures—is a prerequisite to any integration effort. For ICJIS to work, participating criminal justice agencies must agree on, and abide by, a common suite of standards. The ICJIS program will serve as a focal point for cooperative agreement on a complete set of standards needed to realize the integrated justice vision.

The key responsibilities of the standards development component include:

- Establishing enterprise-wide requirements for technical, data, and process standards within the Virginia criminal justice community.
- Coordinating the adoption of standards necessary for effective information integration among Virginia criminal justice agencies.
- Coordinating with other ongoing standards efforts at the state, federal, and international levels, to ensure long-term standards compatibility.

In leading this effort, ICJIS will coordinate with an ongoing initiative of the COTS to define a statewide Enterprise Architecture. The primary goal of the COTS initiative is to establish processes, standards, and a technical infrastructure that will position the Commonwealth to apply and fully exploit technology in the priority business activities of state government.

2.3.4 Data Quality Improvement

For integration to succeed, shared data must be accurate and complete. This poses a significant challenge when some agencies continue to use paper as a primary means to store and share information, coupled with the legacy of stovepipe systems as described in Section 2.1. For ICJIS to work, participating agencies must agree to work together to improve data quality. The ICJIS program can assist agencies by coordinating a statewide effort focused on identifying the causes of poor data quality and taking corrective action.

The key responsibilities of the data quality improvement component include:

- Through cooperative inter-agency efforts, developing requirements and standards that define how certain types of data should be represented.
- Conducting data quality audits including audits of processes that may contribute to data quality problems.
- When funding is available, issuing grants to agencies to address data quality problems.

The challenges related to data quality are not unique to Virginia's criminal justice system. Many other states face the same challenges. Because of the high degree of dependence criminal justice agencies have upon each

other, a coordinated response to these challenges, in parallel with the development of an integrated criminal justice system, has the best chance of success.

2.3.5 System Engineering

As will be discussed in Section 5, ICJIS is not a system in the traditional sense. Rather, it is more properly a technological infrastructure linking together cooperating but independent agency information systems. To implement the technical solutions to the integration problem, someone must design and implement that infrastructure. In addition, someone must help each agency update its information systems to be able to interface with that infrastructure and begin to exploit its capabilities.

The ICJIS program will provide system engineering management services to design and implement the ICJIS infrastructure and the agency interfaces. The key responsibilities of the system engineering component include:

- Designing and developing statewide integration infrastructures for hardware, software, and communications.
- Designing and implementing statewide information system resources needed to facilitate sharing of information across agency and jurisdictional lines.
- Developing recommendations for improvements to existing agency systems that will facilitate greater integration.
- Evaluating and recommending agency adoption of emerging technologies and techniques that may facilitate enterprise-wide integration of information.

2.4 Program Benefits

ICJIS implementation will provide programmatic benefits to operational staff, managers, and decision-makers at all levels of state and local government. Figure 2.4-1 illustrates in a general way the range of potential ICJIS users, the types of benefits they will realize, and the types of information to which they will have improved access.

The following paragraphs present the same information in a much more detailed and specific manner. Provided are specific examples of benefits that will be realized by each specific type of user. Of course, actual benefits will be realized as priorities, funding, and staff resources allow.

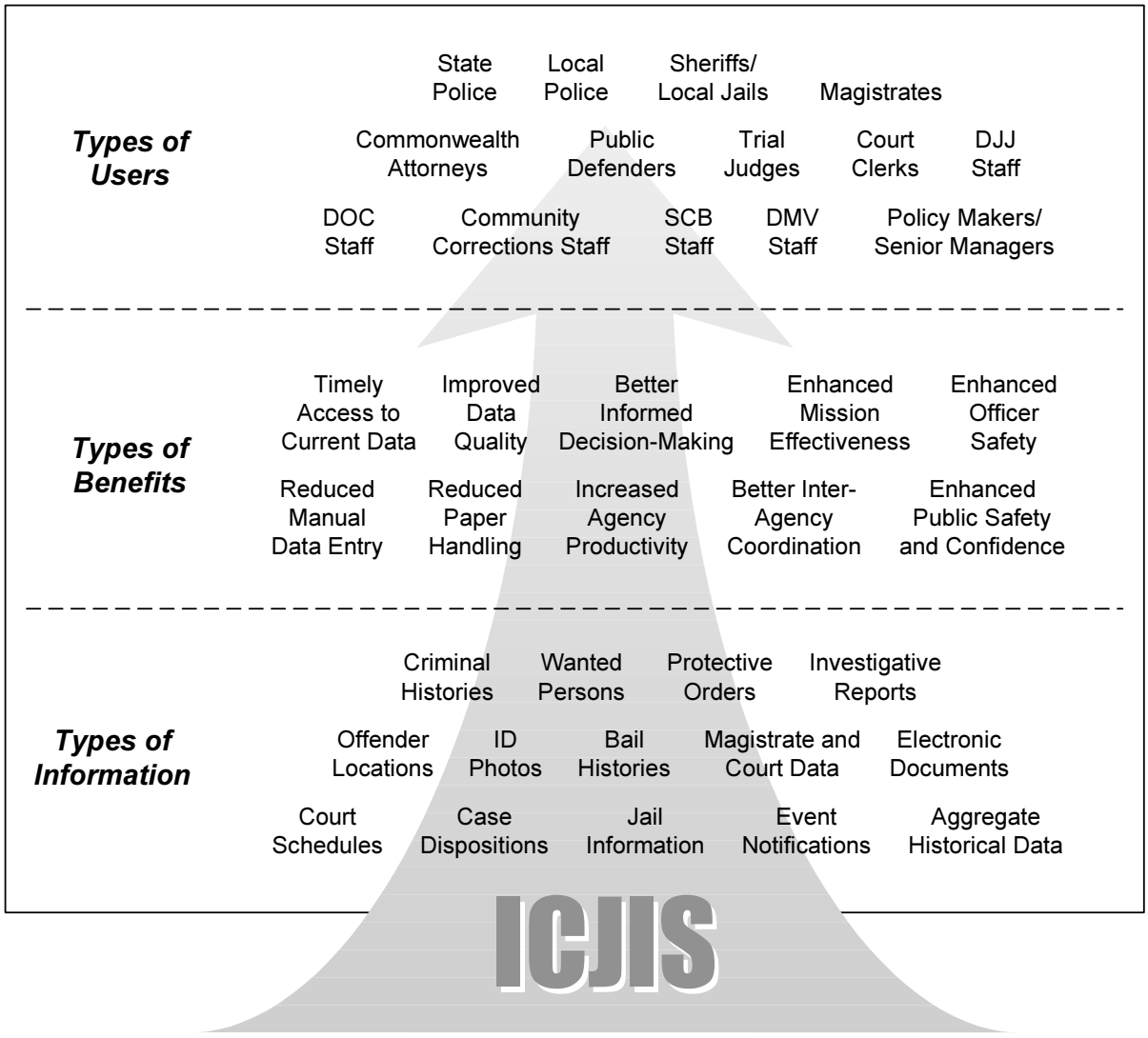

Figure 2.4-1. ICJIS will generate many important benefits to a wide range of users

For state and local police and sheriffs

Better informed decision-making and improved officer safety through:

- More complete and accurate criminal histories. This would help police and sheriffs make better decisions related to police investigations, jail placements, and other activities.
- Wanted persons information updated in real-time. This would allow police to pick up more wanted persons and reduce the chances that someone previously wanted would be picked up on an old warrant.
- Protective order information kept complete and updated in real-time. This would allow for the more effective enforcement of protective orders.

- Availability of current information to help locate persons who are already involved with the criminal justice system (e.g., in another part of the state).
- Enhanced ability to identify people through more efficient sharing of mugshot and DMV photos (building upon initiatives already started in this area).

Agency productivity would be increased through reduced paper handling, and reduced manual data entry in a variety of systems:

- Reduced manual data entry into CCH (the centralized criminal history repository) by providing more reliable court-CCH interfaces and quality control mechanisms.
- Reduced time spent by the state police researching problems related to CCH updates.
- Reduced manual data entry in police and sheriff systems by providing automated interfaces to magistrate and court data. Also, information would be more timely.
- Reduced manual data entry in booking systems by providing automated interfaces to magistrate and court data.
- Reduced manual data entry in wanted persons and protective order systems due to new court to state police system interfaces.
- Reduced manual entry in personal service tracking systems by providing automated access to magistrate and court data. Also, information would be more timely.
- Reduced manual data entry in jail systems by providing automated interfaces to magistrate and court data.

Improved workflow and enhanced productivity through:

- Improved coordination of case processing with courts (e.g., relating to court scheduling, personal service of documents), through automated access to court data statewide.
- Automated tracking of defendants who need to be transported between jails and courts.

- More accurate and timely jail status information (e.g., relating to charging and dispositional information). This is primarily a productivity benefit because less time would be needed to track down correct information.
- Data standards that would allow court order data to be automatically entered into jail systems more quickly and accurately. This would provide a wide range of benefits related to sentence order calculations and productivity improvements.

For magistrates

Better informed decisions through:

- Access to new bail history information. Bail history would inform magistrates when defendants appeared and failed to appear for court hearings in the past, and special conditions that were placed on a defendant in the past and whether the defendant complied with those special conditions.
- Better access to court data. When defendants are currently active in a court, it would be helpful to magistrates to know more about the activities associated with those cases so that new activities can be appropriately scheduled. This access would be provided by either ICJIS or court automated systems.
- Improved criminal history records. When criminal records are incomplete, magistrates do not have access to information critical to bail determination.
- Enhanced ability to verify identities through more efficient sharing of mugshot and DMV photos (building upon initiatives already started in this area).

Improved productivity through:

- Reduced data entry by being able to pull relevant data from DMV and CCH.
- Reduced paper handling through the use of electronic documents.
- Elimination of requirement to create and handle diskettes to send information to courts and others.

For Commonwealth attorneys and public defenders

Better informed decisions through:

- Access to new bail history information to help attorneys decide how to proceed with bail issues.
- Better access to all court data statewide. This would allow attorneys to better coordinate cases across jurisdictions. This access would be provided by either ICJIS or court automated systems.
- Improved criminal history records. Critical decisions are made based on defendant's criminal history. Missing records can cause errors.
- Electronic notification of all new cases and other important events (arrests on warrants, capiases, etc.), prioritized as needed by the local office. Currently attorneys do not know about important events until a defendant appears in court. Electronic notification would allow attorneys to better prepare for important hearings.

Increased productivity through:

- Reduced manual data entry of data that is already available in the courts' automated systems.
- Reduced handling of paper documents since documents would be processed electronically.
- Easier access to court information statewide.
- More efficient case scheduling processes. Currently case scheduling is very labor intensive and would benefit from an inter-agency scheduling system.

For trial judges and clerks

Better informed decisions through:

- Access to new bail history information. This would provide judges with summary information related to a defendant's appearance rate in the past.
- Better access to court data statewide. This would allow judges to better coordinate cases with other jurisdictions.
- Improved criminal history records. This information is critical for bail determination and sentencing.
- Enhanced ability to verify identities through more efficient sharing of mugshot and DMV photos.

Increased productivity through:

- A new electronic filing system for recording new charges, which would reduce data entry.
- More efficient case scheduling and coordination processes.
- Automated tracking of defendants who need to be transported between jails and courts.
- More efficient tracking of personal service processes through an automated interface with sheriffs.
- Reduced telephone calls into courts because staff at other agencies have easier access to court data.

For Department of Corrections (DOC) staff

Enhanced mission effectiveness and coordination through:

- Better access to court data statewide. This would allow DOC staff to better coordinate processing of prisoners and to assist with jail transportation.
- Automatic notifications to probation and parole staff of potential violations of court orders.

Improved data quality and agency productivity through:

- Data standards that would allow court order data to be automatically entered into DOC systems. This would provide a wide range of benefits related to sentence order calculations, staff productivity, and data accuracy.
- Electronic filing of court documents, which would also help to improve timeliness of court filings.
- More accurate and timely entry of information into systems that serve victims.

For State Compensation Board (SCB) staff

The benefits described above related to jails would also be applicable to SCB.

Data quality improvements would allow for more accurate cost reimbursements.

For Department of Motor Vehicles (DMV) staff

Improved coordination through better access to court data statewide. This would allow DMV staff to better prepare for and coordinate administrative hearings with court dates.

Persons convicted of vehicle-related crimes who lose the privilege of driving will not be inadvertently issued driver's licenses because conviction data is not timely entered.

For Department of Juvenile Justice (DJJ) court services and detention staff

Enhanced mission effectiveness and coordination through:

- Better access to court data statewide. This would allow court services and detention staff to better coordinate cases statewide.
- Improved criminal history. This information is critical for many decisions.
- Enhanced ability to verify identities through more efficient sharing of mugshots and DMV photos.
- Automatic notifications to probation staff of potential violations of court orders or agency dictates.

Improved data quality and agency productivity through:

- Data standards that would allow court order data to be automatically entered into DJJ systems. This would provide a wide range of benefits related to sentence order calculations, staff productivity, and data accuracy.
- Electronic filing of court documents, which would also help to improve timeliness of court filings.

For some local corrections programs

Enhanced mission effectiveness and coordination through:

- Better access to court data statewide. This would allow corrections staff to better coordinate cases statewide.
- Improved criminal history. This information is critical for many decisions.
- Enhanced ability to verify identities through more efficient sharing of mugshots and DMV photos.
- Automatic notifications to probation staff of potential violations of court orders.

Improved data quality and agency productivity through:

- Data standards that would allow court order data to be automatically entered into agency systems. This would provide a wide range of benefits related to sentence order calculations, staff productivity, and data accuracy.
- Electronic filing of court documents, which would also help to improve timeliness of court filings.

For policy makers and senior managers

Better informed decisions through:

- More complete, accurate, and timely reports and analyses due to access to more complete, accurate, and timely underlying data.
- An enterprise view of criminal justice processes and data, linked via a standardized data dictionary, regardless of which agencies are providing the data.
- Identification of new opportunities to fundamentally improve criminal justice processes, through access to improved analytical tools and data.

For the general public

The lifeblood of the criminal justice system is information. As information becomes more accurate and timely, criminal justice decision-making will be improved, resulting in:

- Enhanced public safety.
- Increased public confidence in the criminal justice system.

3. Business Problem Analysis

Section Overview

Purpose: To summarize findings of a DCJS analysis of specific business problems regarding information sharing and management within the Virginia criminal justice community.

Key Points:

- As an indicator of the scope of the information management problem, DCJS has identified 37 distinct major steps in the processing flow of a "typical" adult felony case, from investigation of a crime through arrest, prosecution, trial, corrections, and post-corrections activities.
- Each step in the case processing flow may involve multiple agencies collecting and generating information that would be useful to other agencies. Yet most information is shared via manual, hardcopy interfaces, or in some cases not shared at all. Although individual agencies have taken the initiative to implement selective automated interfaces in recent years, there are still relatively few on-line or fully automated data interfaces between agencies.
- This situation results in serious information management problems and shortcomings affecting the entire criminal justice community. DCJS has identified specific examples under five categories of problems: Data Accessibility, Data Standards and Linkage, Data Quality, Inter-Agency Coordination, and Aggregate Analysis.

To better understand the nature of the information integration problem, DCJS has undertaken a detailed business problem analysis of the Commonwealth's criminal justice system. Over a period of many months, the ICJIS program team has conducted surveys and has interviewed representatives and subject matter experts at the major criminal justice agencies.

A critical point to understand is that the integration problem is not merely a technological one. The design of existing information systems goes hand in hand with the design of the human business processes those systems support. In most cases, the operational interface requirements of these systems are woven into the day-to-day activities of criminal justice system workers.

Any evaluation of integration problems between agency information systems must be conducted in the context of the human business processes those systems support. Similarly, to evaluate potential solutions, one must consider the changes that would be required not only to each agency's database systems, but to agency business processes as well.

3.1 Criminal Justice System Workflow: the Adult Felony Example

To give the reader some idea of the scope and complexity of the information integration problem, Figure 3.1-1 shows in step-by-step tabular form how a typical adult felony case is processed by the Virginia criminal justice system. Each step in the table is a significant but discrete event in the handling of a case by one or more agencies of the criminal justice community.

The transition from one step to the next is typically a point at which responsibility for case processing is passed from one agency to another. It is also a point at which critical information must be passed to, or collected by, the receiving agency from the agencies and steps that have gone before.

In the table, we have identified the most important information inputs required at each step, along with the most significant information outputs. Following each input and output, we have indicated whether that information is currently passed in manual (M), interactive (I), or fully automated (A) form.

By manual (M), we mean that the information is stored and/or accessed in non-digital form, typically as a hardcopy document, but in some cases even as verbal communication. By interactive (I), we mean that the person generating the information manually enters it on a workstation for storage in a computerized database, and/or that the recipient of the information obtains it via a manually entered inter-agency query. A critical limitation of interactive inter-agency interfaces is that, if the recipient wishes to store some of the retrieved information into his/her own database system, he/she must manually re-enter the data through a separate interactive interface. This problem is solved by fully automated (A) interfaces, through which the transfer of information from agency to agency is performed automatically by cooperating computer systems, with no manual intervention required.

Event	Agencies/ Persons	Inputs	Outputs
1. Police investigate crime.	Investigating police agency; Other police agencies; Suspects; Victim; Witnesses; Forensics; Others	Evidence (M); Forensics (M); Witness statements (M); Fingerprint matches (M or I); Criminal histories (I); Mugshots (M); DMV information (I); DMV photos (M); Prior police reports (M, I or A); Police investigative files from other agencies (M)	New police reports (M or I); IBR update (M or I); Updates to local police investigative files or systems (M or I)
2. Probable cause determined. Magistrate issues arrest warrant.	Magistrate; Investigating police agency; Victim	Verbal complaint (M); Criminal history of suspect (M)	Arrest warrant (I)

Event	Agencies/ Persons	Inputs	Outputs
3. Local police enter warrant into wanted persons system.	Local police agency; VSP	Arrest warrant (M)	Wanted persons record (I)
4. Suspect arrested.	Arresting police agency; Police agency holding warrant; Suspect	Wanted persons record (I); Manual confirmation of warrant (M); Arrest warrant (M); Criminal history (I); DMV information (I)	
5. Magistrate confirms identity of defendant, conducts bail hearing, sets bail require-ments. Defendant cannot meet bail require-ments.	Magistrate; Arresting police agency; Defendant	Arrest warrant (M); Criminal history (M); DMV information (M); Police arrest information (M); Defendant statements (M); Court records (M)	Updated arrest warrant (I); Commitment order (I)
6. Local police enter warrant execution information into wanted persons system.	Local police agency	Arrest warrant (M)	Updated wanted persons record (I)
7. Booking.	Booking agency; Arresting police officer; Defendant	Arrest warrant (M); Commitment order (M)	SP-180 information including fingerprints (M or I); Mugshots (M or I); SID (if automated interface with VSP) (A)
8. Update local police system with investigative and/or criminal history information.	Local police agency	Arrest warrant (M); Other information generated by magistrate (M); SP-180 information (M, I, or A); Mugshots (M or A); SID (M or A)	Updated police records (M and I)

Event	Agencies/ Persons	Inputs	Outputs
9. Jail intake and commitment.	Jail intake; Defendant; Arresting police officer	Arrest warrant (M); Commitment order (M); Defendant statements (M)	Commitment/release information—specifics on how this information is managed varies between jails (M and I)
10. Community Corrections bail assessment.	Community Corrections (local); Defendant	Arrest warrant (M); Commitment order (M); Criminal history (I)	Bail recommendation (M)
11. Court intake.	Court intake	Arrest warrant (M and A); Commitment order (M and A); Other information generated by magistrate (M and A)	CAIS records updated (I)
12. General District Court arraignment. Bail conditions modified. Defendant posts bond.	Judge/clerk; Commonwealth Attorney; Defendant	Arrest warrant (M and A); Commitment order (M and A); Other information generated by magistrate (M and A); Bond information provided by defendant (M)	Updated arrest warrant (M); Recognizance (M); Receipt (I and A); Release Order (M); CAIS records updated (I); Financial statement for public defender (M)
13. Defendant meets with public defender.	Public defender/ clerk; Defendant	All court documents (M)	Public defender intake—specifics on how this information is managed varies between offices. (M or I); Public defender enters their appearance on case (M)
14. Preliminary hearing. Probable cause established. Charges certified.	Judge/clerk; Commonwealth Attorney; Public Defender; Defendant.	All court documents (M)	Updated arrest warrant (M); CAIS records updated (I)
15. Common-wealth Attorney prepares and files with court an indictment.	Commonwealth Attorney; Court clerk	All court documents (M); Police report (M or A)	Indictment (M or I)

Event	Agencies/ Persons	Inputs	Outputs
16. Circuit Court intake.	Court clerk	Indictment (M); All court documents (M and A)	CAIS records created for Circuit Court (I)
17. Grand Jury. Probable cause established. True bill issued.	Commonwealth Attorney; Grand jury; Judge/clerk	Indictment (M)	True Bill (M); CAIS records updated (I)
18. Circuit Court arraignment. Defendant pleads not guilty.	Judge/clerk; Commonwealth Attorney; Public defender; Defendant	All court documents (M)	Updated arrest warrant (M); CAIS records updated (I)
19. Pre-trial activities (bail review, scheduling, evaluations, summoning, jury selection, etc.)	Judge/clerks; Commonwealth Attorney; Public defender; Sheriff (personal service); Defendant; Victim; Others	All court documents (M and A)	Various court documents depending on the circumstances (M and/or I)
20. Attorneys prepare for trial.	Commonwealth Attorney; Public defender; Defendant; Victim; Witnesses; Police	All court documents (M); Police report (M or I); Criminal history (I); Defendant statements (M); Victim statements (M); Witness statements (M); Police statements (M)	Motions and other filings (M); Amendments to charges (M); Plea agreements (M); Summons issued by attorneys (M or I)
21. Trial.	Judge/clerk; Jury; Commonwealth Attorney; Public defender; Defendant; Victim; Witnesses; Police; Sheriff	All court documents (M); Plea agreements (M); Summons issued by attorneys (M or I)	Evidence (M); Testimony (M, I, or A); Updated arrest warrant (M); Order for pre-sentence report and/or victim impact assessment (M); CAIS records updated (I); Work schedules (M)

Event	Agencies/ Persons	Inputs	Outputs
22. Pre-sentence or some other type of background investigation or assessment, and victim impact.	DOC; Offender; Victim; Others	Order for pre-sentence report and/or victim impact assessment (M); Criminal history (I); Prior evaluations (M); Defendant statements (M); Victim statements (M); Other documents (M)	Pre-sentence report (M); Victim impact (M)
23. Sentencing.	Judge/clerk; Commonwealth Attorney; Public defender; Offender; Victim	Pre-sentence report (M); Victim impact (M); All court documents (M and I); Post-sentence reports (M)	Testimony (M, I, or A); Updated arrest warrant (M); Sentence order (M and I); CAIS records updated (I)
24. CCH updated per CCRE procedures. Disposition and sentencing information is sent after appeal period ends.	Courts; VSP	CCRE information (A)	CCRE information (A)
25. DMV update if charges relate to motor vehicles.	Courts; DMV	DMV information (A)	DMV information (A)
26. Defendant sent to jail awaiting transfer to DOC.	Jail; Offender	Sentence order (M)	
27. Prison.	Jail; DOC; Offender	Papers from jail file (M); Sentence order (M); Pre/post-sentence investigations (M); Pre/post-sentence reports (M)	DOC records updated (M and I)
28. CCH updated per CCRE procedures. DOC sends offender status changes.	DOC; VSP	CCRE information (A)	CCRE information (A)

Event	Agencies/ Persons	Inputs	Outputs
29. Transfer to probation.	DOC; Offender	Papers from prison (M); Sentence order (M)	DOC records updated (M and I)
30. CCH updated per CCRE procedures. DOC sends offender status changes.	DOC; VSP	CCRE information (A)	CCRE information (A)
31. Probation violation. Arrest document filed by probation officer.	DOC; Court clerk	Arrest document filed with court (M)	Court orders arrest (M and I)
32. Local police update wanted persons system.	Local police agency; VSP	Arrest order (M)	Updated wanted persons system (I)
33. CCH updated per CCRE procedures. DOC sends offender status changes.	DOC; VSP	CCRE information (A)	CCRE information (A)
34. Offender arrested. Local police update wanted persons system.	Arresting police agency; Police agency holding arrest document; Offender	Arrest order (M); Manual confirmation of arrest document (M)	Updated wanted persons system (I)
35. Offender appears in court. Offender is given maximum sentence and ordered back to prison.	Judge/clerk; Commonwealth Attorney; Public defender; Offender	Papers from probation file (M); Sentence order (M); Criminal history (I)	DOC records updated (M and I)

Event	Agencies/ Persons	Inputs	Outputs
36. Offender is released after serving sentence.	DOC; Offender	Calculated release date (M and I)	DOC records updated (M and I)
37. CCH updated per CCRE procedures. DOC sends offender status changes.	DOC; VSP	CCRE information (A)	CCRE information (A)

Note 1. For each court appearance while the defendant is in jail or prison, the defendant's transportation needs to be coordinated between the courts, jails, and DOC. Also, transportation between corrections facilities needs to be coordinated.

Note 2. Local police systems may receive dispositional and sentencing information from the courts, depending on local agreements.

Figure 3.1-1. Step-by-Step Processing of a Typical Adult Felony Case

As can be seen, the scope of the information management problem is vast, encompassing many different users at many agencies with requirements to collect many different kinds of information, almost all of which must be shared at some point in the process. Unfortunately, the vast majority of information transfers between agencies are currently performed manually. There are several important and very valuable interactive interfaces. However, there are very few interfaces that qualify as fully automated.

From a business process engineering standpoint, each information transfer that is less than fully automated represents an opportunity for errors, redundant effort, and delays to be introduced into the criminal justice system. When one multiplies the interfaces times the number of adult felony cases handled each year (roughly 100,000), the number of problem opportunities becomes quite daunting. When one further takes into account the many other types of criminal justice cases other than adult felonies (misdemeanors, traffic offenses, juvenile offenses, domestic relations cases, protective orders, etc.), then the total number of problem opportunities becomes staggering.

An additional complicating factor is that not all events in the criminal justice system occur in the orderly, step-by-step manner that may be suggested by Figure 3.1-1. In real life, events sometimes occur out of order. For example, police may respond to an emergency call and arrest a suspect at a crime scene before a magistrate has issued an arrest warrant. Or the police may uncover new evidence partway through the presentation of a Commonwealth Attorney's case in court that changes how the case should be processed. Any inter-agency information sharing process must have the flexibility to handle exceptions and special cases as well as the nominal standard workflows.

3.2 Current Problems and Shortcomings

By analyzing the information collected during our business problem analysis, DCJS has identified five general categories of information problems or shortcomings that may be attributed to lack of sufficient integration:

- Data Accessibility
- Data Standards and Linkage
- Data Quality
- Inter-Agency Coordination
- Aggregate Analysis

Each of these problem areas is discussed in the subsections below.

3.2.1 The Data Accessibility Problem

Figure 3.2.1-1 is a table showing examples of cases where a particular agency possesses data that would be highly useful to other agencies but which are not currently directly accessible by those other agencies.

3.2.2 The Data Standards and Linkage Problem

In some situations, even when it is technically feasible for one agency to share information with another agency's database, differences in data formats or retrieval keys may make it very difficult to logically relate data from the two systems. Figure 3.2.2-1 lists examples of specific problems in this area.

Data	Accessibility Problems
Booking status information held by VSP	Data are not accessible to the courts, who need to know in real-time if a defendant has been booked for a specific charge.
Charge data held by courts	Data are not accessible by courts other than the one where the charges are active. Also not accessible to other criminal justice agencies.
Commitment/release and location information held by corrections agencies	Data are not accessible to other corrections agencies, police, Commonwealth Attorneys, courts, and defense attorneys.
Defendant data on active cases, held by the courts	Data are not accessible by courts other than the one where the charges are active. Also not accessible to other criminal justice agencies.
Court data in general	Data not accessible statewide to all criminal justice professionals, including court staff, and not available locally to most criminal justice professionals who occasionally need this data.
DMV photos and driver physical characteristics	The DMV currently provides criminal justice agencies with on-line access to driving records, restrictions, suspensions, and license data. However, DMV does not support on-line access to current photos or driver physical characteristics, which would be highly useful to police, commonwealth attorneys, courts, and corrections agencies.

Figure 3.2.1-1. Examples of Data Accessibility Problems

Data	Data Standards and Linkage Problems
Bail conditions	This data is generated by magistrates and the courts but cannot be linked to offender records at VSP and police systems.
Bail history	This data is held by magistrates and courts but cannot be linked to offender records at magistrates and courts in other jurisdictions.
Charge identification and charging data	There is no standard unique identifier for tracking a charge across agency systems that is applicable in all situations. This creates various problems in keeping CCH and other systems updated.
Defendant/offender identification	Beyond CCRE, there are no standardized rules on the use of SIDs and non-fingerprint-based unique identifiers. This makes it very difficult to link data about a defendant/offender when no common SID is available.
Defender/offender locate data	Offender location data is spread throughout the criminal justice system with no way to link the data or determine currency. There is no automatic way to link a change of address at one agency to records about the same individual at other agencies.
Filing of new charges of special interest to the Commonwealth Attorney	This data is held by the courts but is not linked to active files at the local Commonwealth Attorney's office.
Filing of new charges related to offender on probation or parole	This data is held at the courts but is not linked to systems used by probation/parole staff at DOC and DJJ.
Mugshots	Local police agencies maintain their own files of mugshots that are not linked by common ID to other police agencies, Commonwealth attorneys, courts, or corrections agencies.
Offender's event history information (regardless of jurisdiction)	This information is scattered across all criminal justice agencies with no common ID available to link it all together.
Offense descriptions (Virginia Crime Codes versus statutes)	Some agencies use VCC codes and others use statutes.
Protective order data	This data is held by magistrates and courts who issue protective orders, but they do not get linked to VSP and local police systems.
Sentence orders	This data is held by the courts, is sometimes incomplete, and is not linked to data held by other courts, jails, DOC, DJJ, Commonwealth Attorneys, and public defenders.
Wanted persons	This data is generated by magistrates and courts but is not linked to systems at VSP and local police agencies.
Common data fields	Most agency database system have independently defined formats for common data fields (e.g., name, address, social security number). Incompatibilities in data formats make it difficult to associate and integrate records across agencies. Agreement on an enterprise-wide common data dictionary is needed.

Figure 3.2.2-1. Examples of Data Standards and Linkage Problems

3.2.3 The Data Quality Problem

Problems in data quality refer to data being incomplete, obsolete, and inaccurate. The impact is that operational staff and decision-makers are forced to make decisions without benefit of all relevant information. Figure 3.2.3-1 lists examples of specific data quality problems.

Data	Quality Problems
Redundant offender and case data entry	Many agencies manually enter the same offender and case information into their computer systems, due to the absence of means for automatically loading data previously captured by another agency. Each time the same data is re-entered, there is an opportunity for introducing errors, omissions, and inconsistencies into the criminal justice system.
Data missing or not captured in computerized information systems	Not all data fields are fully or consistently populated within existing database systems. Some agencies still maintain some critical data on paper, which can lead to outside agencies perceiving that data as missing or incomplete when accessing the databases.
Offender Social Security Numbers	Various criminal justice agencies currently manually capture Social Security Numbers for offenders. However, there are no systematic processes for verifying that these SSNs are accurate. It is widely suspected that a significant percentage of SSNs are in fact bogus.

Figure 3.2.3-1. Examples of Data Quality Problems

3.2.4 Inter-Agency Coordination Problem

There are many cases where lack of integration leads to problems or inefficiencies in inter-agency coordination or workflow. Figure 3.2.4-1 lists some specific examples.

Inter-Agency Event	Limitations in Current Inter-Agency Coordination
Court dispositions and sentences	Some local police agencies want to receive this information automatically. While several interfaces currently work well, processing is still done manually in most jurisdictions.
Court schedules and case status	The scheduling of court cases can be difficult in some jurisdictions where coordinating the schedules of all parties is not automated. Scheduling activities may be managed by both the courts and the Commonwealth Attorneys.

Inter-Agency Event	Limitations in Current Inter-Agency Coordination
Court filings and court documents	The courts are a central component of the criminal justice system. The workload of most criminal justice agencies is dependent on, or driven by, the work of the court. For example, agencies prepare cases for court, file court documents, appear in court, act on court warrants and capiases, respond to court notices, implement court orders, etc. Unfortunately, even with recent advances, most interfaces with the court remain manual and paper-based. Automation of data interfaces would enhance workflow and reduce the burdens of manual coordination and time-consuming copying of paper documents.
Service of documents	Current processes are manual and prone to significant delays.
Event monitoring and management	Agencies and individuals would like to be able to monitor significant events and current status of a particular case, as it proceeds through the many steps of the criminal justice processing cycle. Although each agency has methods for tracking a case in terms of its own activities, there is no way to view the complete sequence and status of events for a case.

Figure 3.2.4-1. Examples of Inter-Agency Coordination Problems

3.2.5 The Aggregate Analysis Problem

Figure 3.2.5-1 shows examples of the types of historical and statistical data analyses that would be useful but cannot currently be performed, due to lack of access to data aggregated from multiple agencies. The examples cited are intended to be purely illustrative and are not necessarily being advocated by DCJS.

Type of Analysis	Data Combinations Needed
Impact of special correctional programs (e.g., first offender programs)	Ability to link charges and offenders across multiple databases, along with a way to identify participants in particular programs.
Near-real-time projections of incarceration rates, to support more effective utilization of prison and jail space statewide	Ability to link charges and offenders across multiple databases, along with historical data that can be used to project probability and length of incarceration given certain criteria.
Timeliness of case processing	Ability to link case and event information across multiple databases and generate timeline statistics based on selected criteria.
Workload assessments	Ability to link charges and offenders across multiple databases, along with standards for quantifying workload.

Figure 3.2.5-1. Examples of Aggregate Analysis Problems

4. The Integrated Justice Solution

Section Overview

Purpose: To describe a functional concept of operations for how strategic improvements to business processes and information systems would result in an enterprise-wide solution to the information management problems described in the previous chapter.

Key Points:

- The ICJIS program proposes community-wide adoption of an integration approach based on the SEARCH/NASIRE model—a cooperative model specifically designed for integration of autonomous information systems maintained by independent agencies.
- The SEARCH/NASIRE model defines a set of five integration functions through which independent agency systems may cooperate with each other to share and manage information—Query, Pull, Push, Subscribe/Notify, and Publish.
- The ICJIS program proposes to add a sixth integration function to the basic model—Aggregate Data Assembly and Analysis.
- The ICJIS program has also identified two critical supporting functions that are implicit in the six basic integration functions, and that are mandatory for their successful implementation. These are inter-agency data linking functions for data about individuals and cases.

4.1 Concept of Operations: Integration Functions

Clearly, if the problems discussed in Section 3 are caused by the absence of an integrated approach to data management, then the solutions lie in improving the level of integration in criminal justice data management. The question is how the greater level of integration should be achieved.

After reviewing ongoing integration initiatives at the federal level and in other states, the ICJIS program has determined that the most cost-effective solution lies in the adoption of a modified version of the SEARCH/NASIRE integration model described in Section 2.3. Under the original model—proposed by the SEARCH organization and subsequently adopted by NASIRE, an association of state government chief information technology executives—there are five fundamental information system functions needed to achieve a meaningful level of integration among independent agency systems:

- Inter-Agency On-Line Query
- Inter-Agency Information Pulling
- Inter-Agency Information Pushing
- Inter-Agency Event Subscription and Notification
- Inter-Agency Information Publishing

DCJS's analysis of Virginia business problems led to the addition of a sixth fundamental integrating function to the ICJIS model:

- Inter-Agency Aggregate Data Assembly and Analysis

Each of these functions is discussed in detail in the following subsections. At this stage of analysis, the functions are described in conceptual terms, to give the reader a general idea of their purpose and how they might address known integration problems. A more technical discussion of how these functions may be implemented is given in Section 5.

It is important to understand that, while all of these functions must be supportable by the overall ICJIS architecture, it is not required or expected that they will be implemented immediately or all at once by every agency system. In fact, one of the most appealing aspects of the SEARCH/ NASIRE model is its functional modularity. For example, one agency system may elect to implement some of the functions—e.g., inter-agency on-line query, push, and pull—and defer the rest, while another agency system may choose to implement a different mix, such as inter-agency event subscription and notification, push, pull, and publish. In the long run, of course, the goal is to have all participating systems implement all of the functions.

4.1.1 Inter-Agency On-Line Query

The ICJIS solution should allow an authorized on-line user to query relevant agency database systems for information critical to his/her mission. In many cases, agencies already provide interactive query access to their databases by their own agency users and/or to a limited set of outside users. ICJIS's role will be to facilitate query access to all relevant databases by authorized users at any ICJIS agency. Figures 4.1.1-1 through 4.1.1-3 show different scenarios for how this function might work.

Figure 4.1.1-1 shows how ICJIS would allow a user logged on to an existing system at one agency (Agency 1) to query a database at a different agency (Agency 2). The operational concept is that the Agency 1 user's native host system will be upgraded to provide a query and response interface between its users and the ICJIS network. The role of ICJIS will be to route the query to the appropriate target system and provide any data translation services that may be needed between the two systems. The target system at Agency 2 would have to be upgraded to accept the query from the ICJIS network and to transmit query results back over the network to the requesting system.

Figure 4.1.1-2 shows an alternate scenario in which the Agency 1 user's query is routed to a central ICJIS server rather than to an existing agency system. Under this scenario, the ICJIS would maintain some databases independent of existing agency systems. There are several general situations in which this may occur:

- In some cases, agencies have expressed reluctance to opening up a particular system to on-line queries from outsiders, due to system performance or security concerns. In such cases, it may be possible to create and maintain a copy of the agency database—with sensitive and proprietary data eliminated—and place it on an ICJIS server for outsiders to query.
- To make data easier to access, data from multiple agencies could be copied, transformed in accordance with standards, and integrated into a more

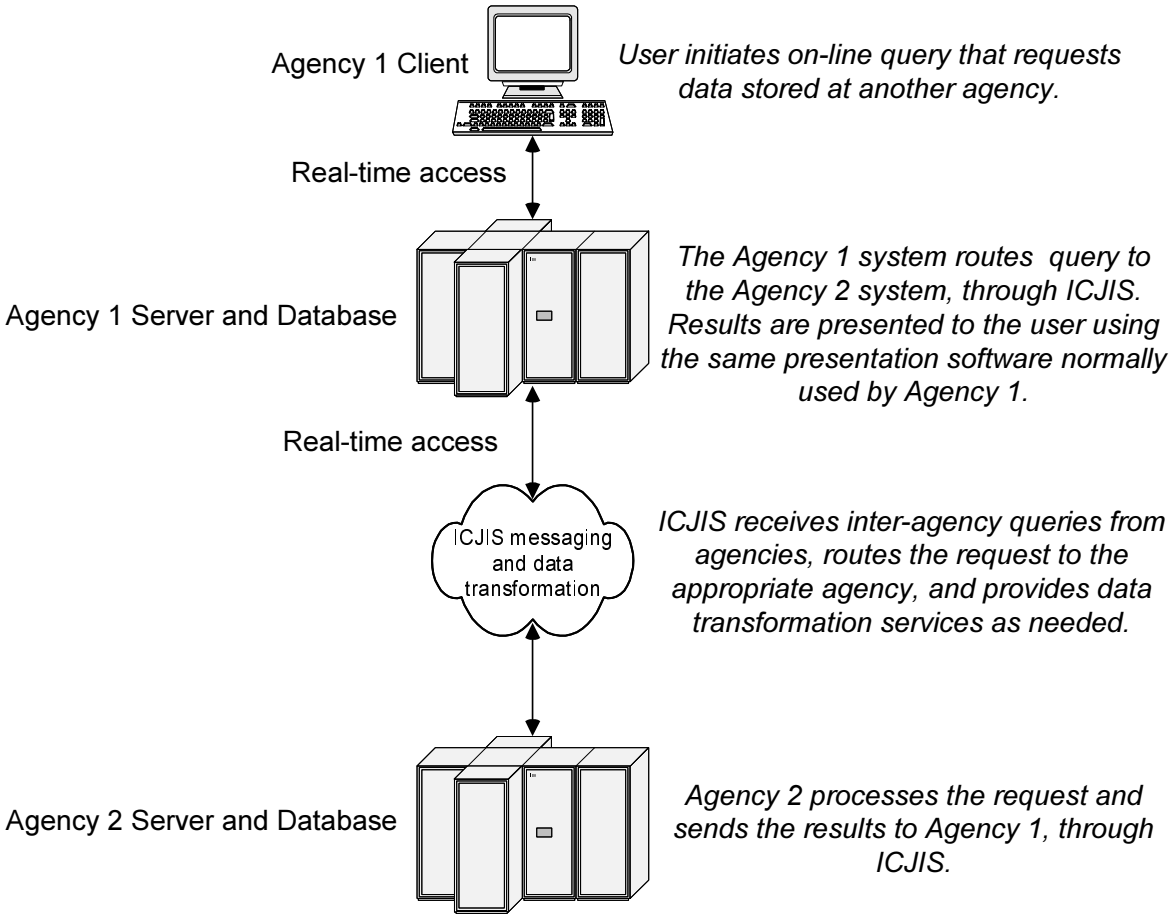

Figure 4.1.1-1. On-Line Query—Scenario One: Agency to Agency

efficient data structure located on an ICJIS server. The database would be structured to meet the needs of the larger community. This would improve the presentation of data as well as overall system performance. For example, event information is maintained many different ways across the agencies. By storing event information on a central database, this allows for more extensive data transformation routines and, to the end user, the data on the screen would look like it is coming from a single system instead of several systems (i.e., it would be faster and more user friendly).

- Having a central ICJIS server would, to a significant degree, protect agencies from changes that may occur at other agencies. For example, if Agency 1 changes its internal database structure or technical environment, all other agencies accessing data from Agency 1 would potentially have to make database and/or software changes to remain in synch. With ICJIS serving as a central buffer, changes at Agency 1 could be accommodated by changes to the ICJIS interface with Agency 1, and none of the other agencies would be affected. This would make it easier for all agencies to manage their internal system development and maintenance projects.
- There may be a need for specialized databases that currently do not exist but which would provide great value to users at multiple agencies. Examples include a

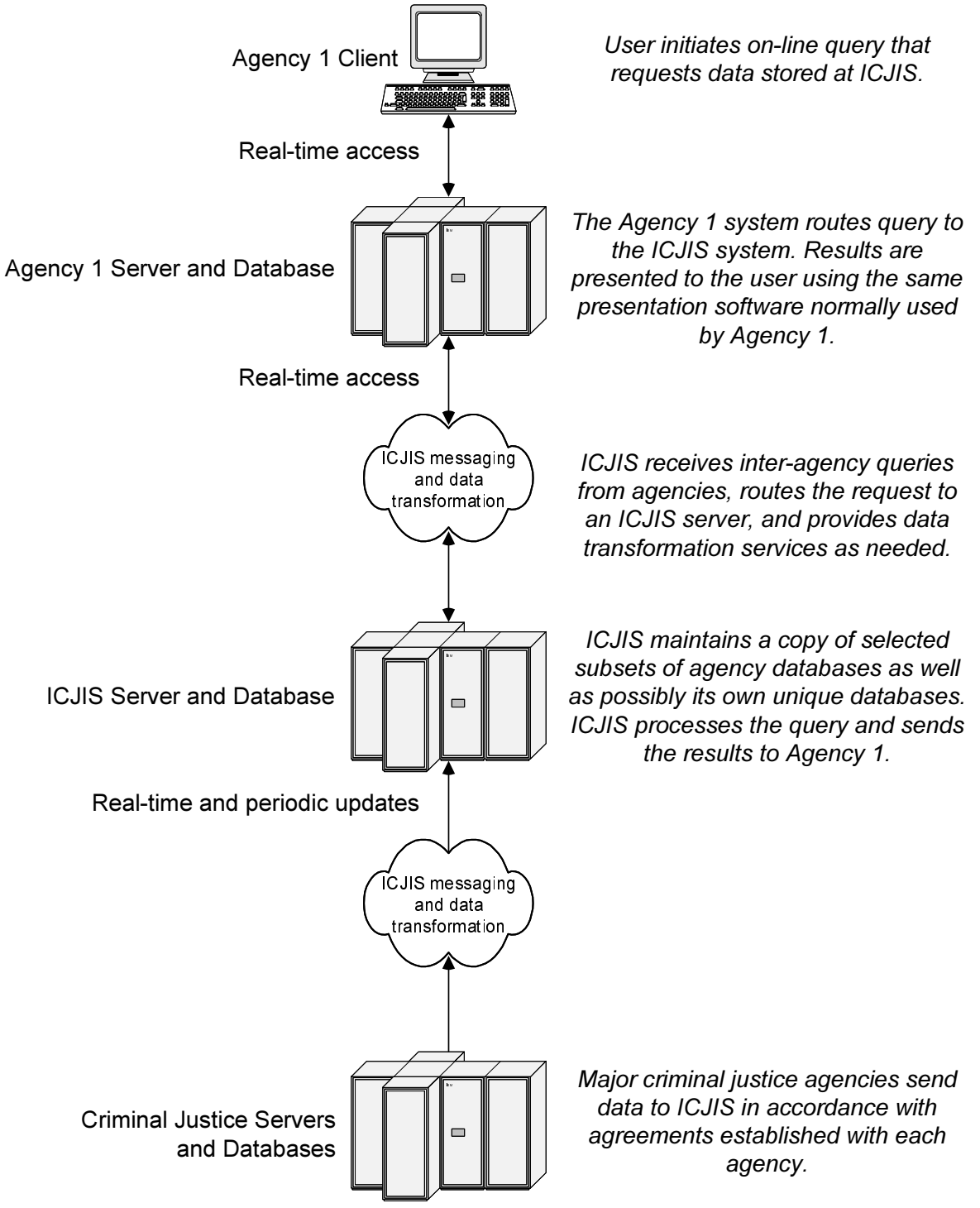

Figure 4.1.1-2. On-Line Query—Scenario Two: Agency to ICJIS

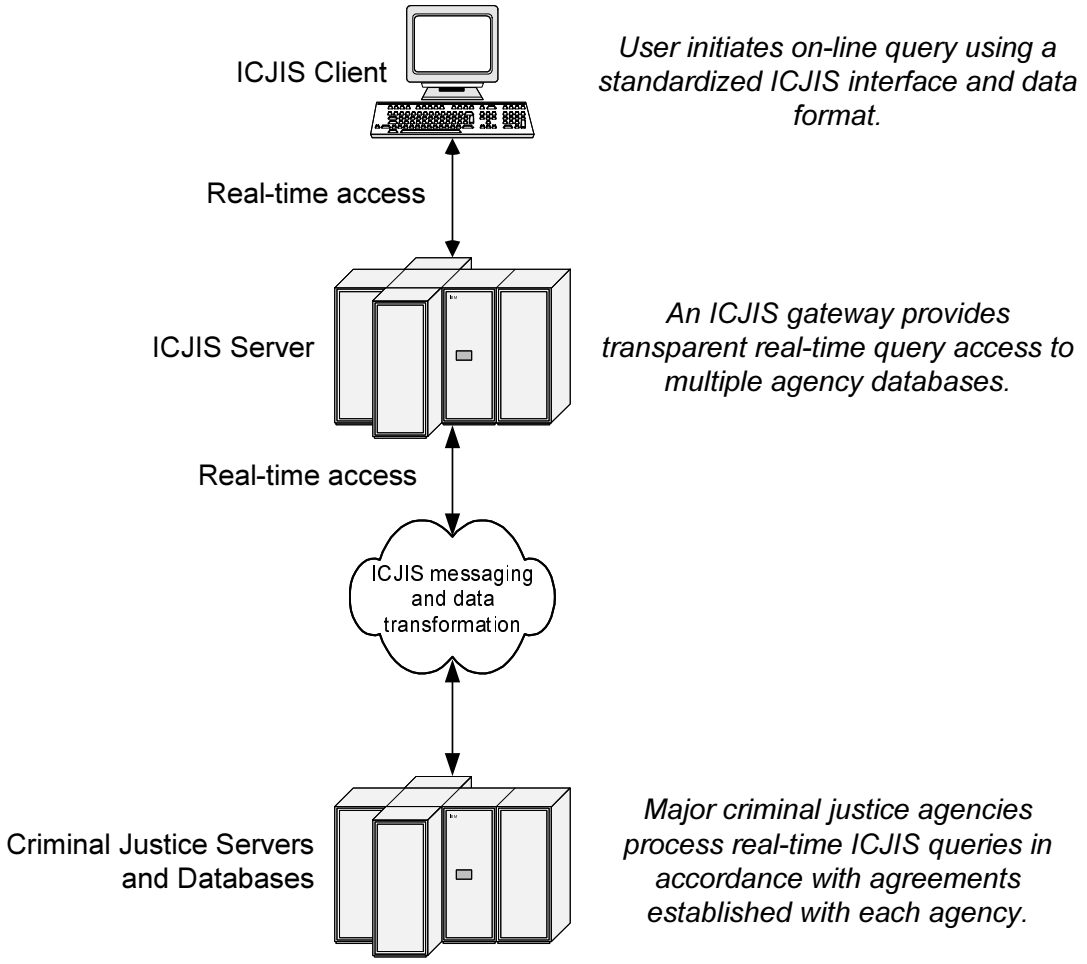

Figure 4.1.1-3. On-Line Query—Scenario Three: ICJIS to Agencies

photograph database, or a database of pointers allowing users to efficiently retrieve photographs stored in agency databases. Pointers are usually numbers that can efficiently link two databases.

As shown in Figure 4.1.1-2, in such cases ICJIS would route the query to itself, and provide the query response. For cases where ICJIS is maintaining a copy of an agency database, the diagram shows a requirement for the agency to provide periodic updates in order to keep the ICJIS copy reasonably current.

Figure 4.1.1-3 shows a third scenario for the on-line query function. Here, the ICJIS itself will provide a common user interface through which an authorized user will have access to databases on the network. As will be discussed further in Section 5, it is likely that many users will access ICJIS through standard desktop PCs rather than through a custom agency-specific workstation interface. For those users, it would be cost-effective for ICJIS to provide a common user interface, perhaps accessible through a web browser.

In this scenario, the ICJIS would serve as a standardized gateway interface to multiple agency host systems. ICJIS would be responsible for translating and routing each user query to the appropriate agency host system(s), or to itself in the case of databases located on a central ICJIS server.

Each of the three scenarios has its pros and cons. The actual ICJIS implementation may be based on a combination or hybrid of the three alternatives.

4.1.2 Inter-Agency Information Pulling

The ICJIS solution should allow an application program running on one agency's system to *pull* (i.e., retrieve) relevant data from databases maintained by other agencies. An example might be a wanted persons or booking application that automatically retrieves relevant data about the charge and the suspect from a magistrate warrants system. Figures 4.1.2-1 and 4.1.2-2 show different scenarios for how this function might work.

Figure 4.1.2-1 shows how an application running on a system in Agency 1, perhaps but not necessarily under the control of a local on-line user, determines that it needs data from one or more systems operated by other agencies. Conceptually, the data pulling scenario is almost identical to the on-line query scenario, except that the information requests are generated by an application program rather than directly by a human user. From the users' point of view, they need not be aware of where the data is located or how to ask for it, only that it shows up on their screens or in their reports when they need it.

Once it determines that it needs data from a particular external system, the application program will generate one or more ICJIS

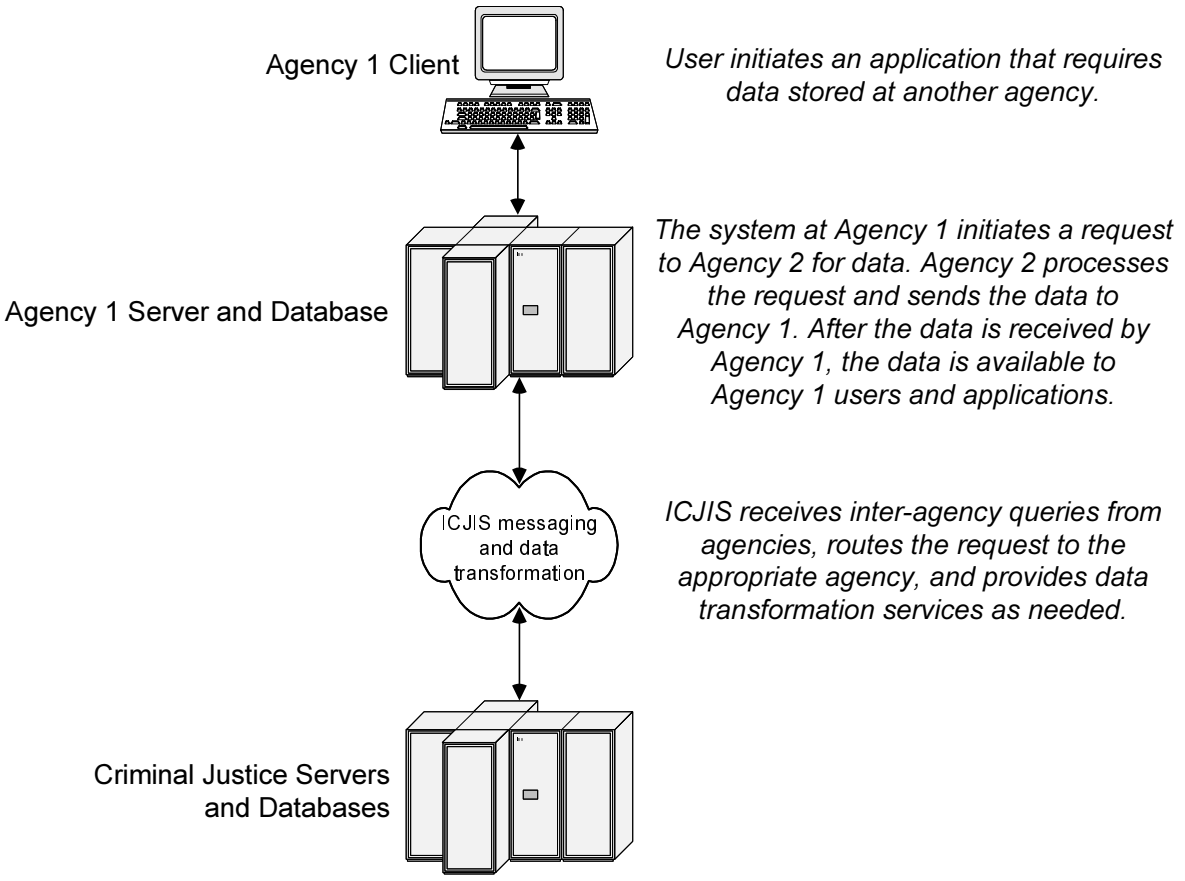

Figure 4.1.2-1. Pull—Scenario One: Agency to Agency

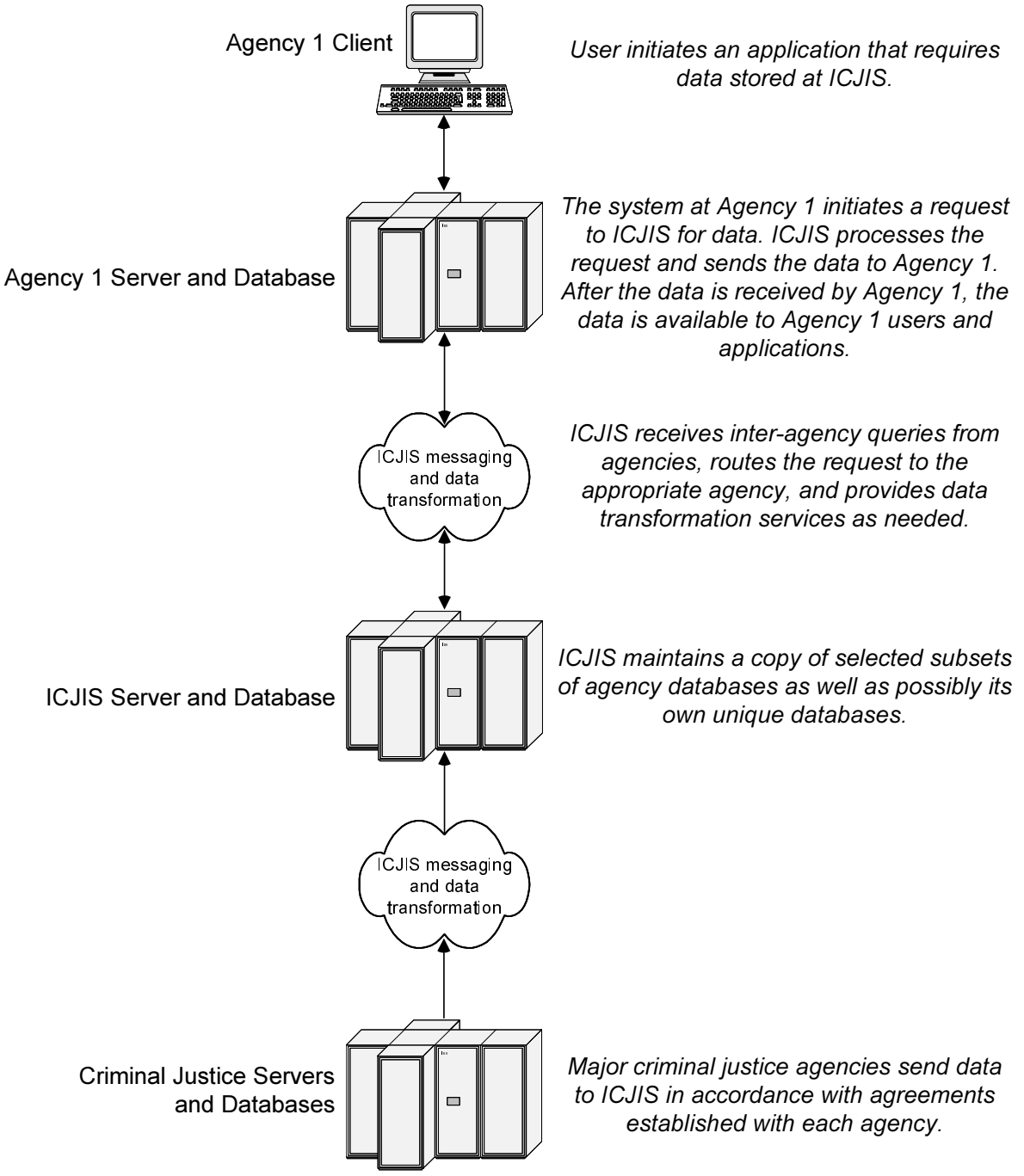

Figure 4.1.2-2. Pull—Scenario Two: Agency to ICJIS

standard queries and pass them to an ICJIS interface module. The role of ICJIS will be to route the queries to the appropriate target system(s) and provide any data translation services that may be needed between the systems. The target systems would process the queries and transmit results back over the network to the requesting application program.

Depending on the implementation, the ICJIS pull interfaces may be implemented entirely on the two cooperating agency hosts, or may involve a central ICJIS server that handles some of the processing on behalf of the agency host systems.

Figure 4.1.2-2 shows the alternate scenario for pulling from a database maintained by ICJIS rather than by an agency system. The same motivations for keeping some databases on a central ICJIS server rather than on an agency system—discussed under the on-line query scenarios—apply here as well. In such cases, ICJIS will route the data pull request to itself and transmit results to the requesting application program.

4.1.3 Inter-Agency Information Pushing

The ICJIS solution should allow an application program running on one agency's system to *push* (i.e., transmit) relevant data to database systems maintained by other agencies. An example might be a booking application that automatically transmits arrest data to the prosecutor's office, where a receiving application initiates a case file. Figures 4.1.3-1 and 4.1.3-2 show different scenarios for how this function might work.

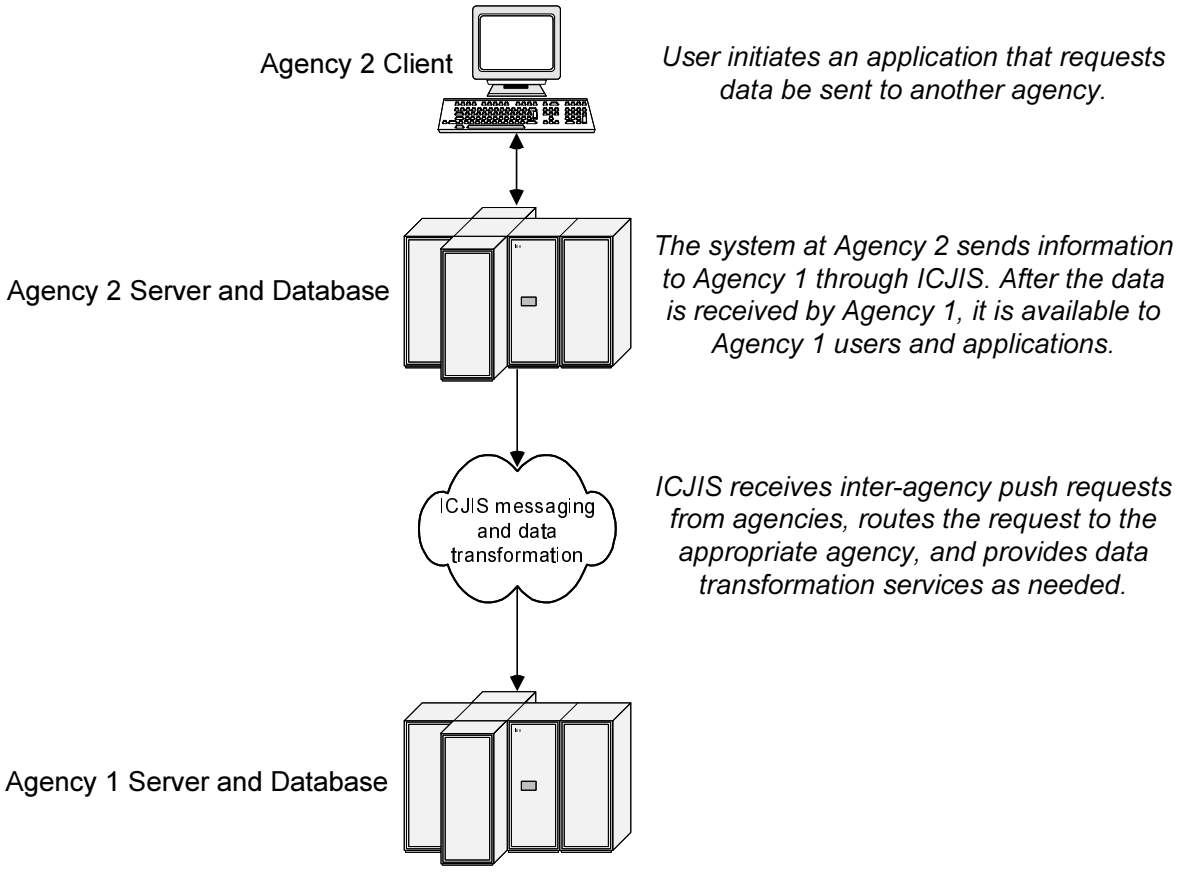

Figure 4.1.3-1. Push—Scenario One: Agency to Agency

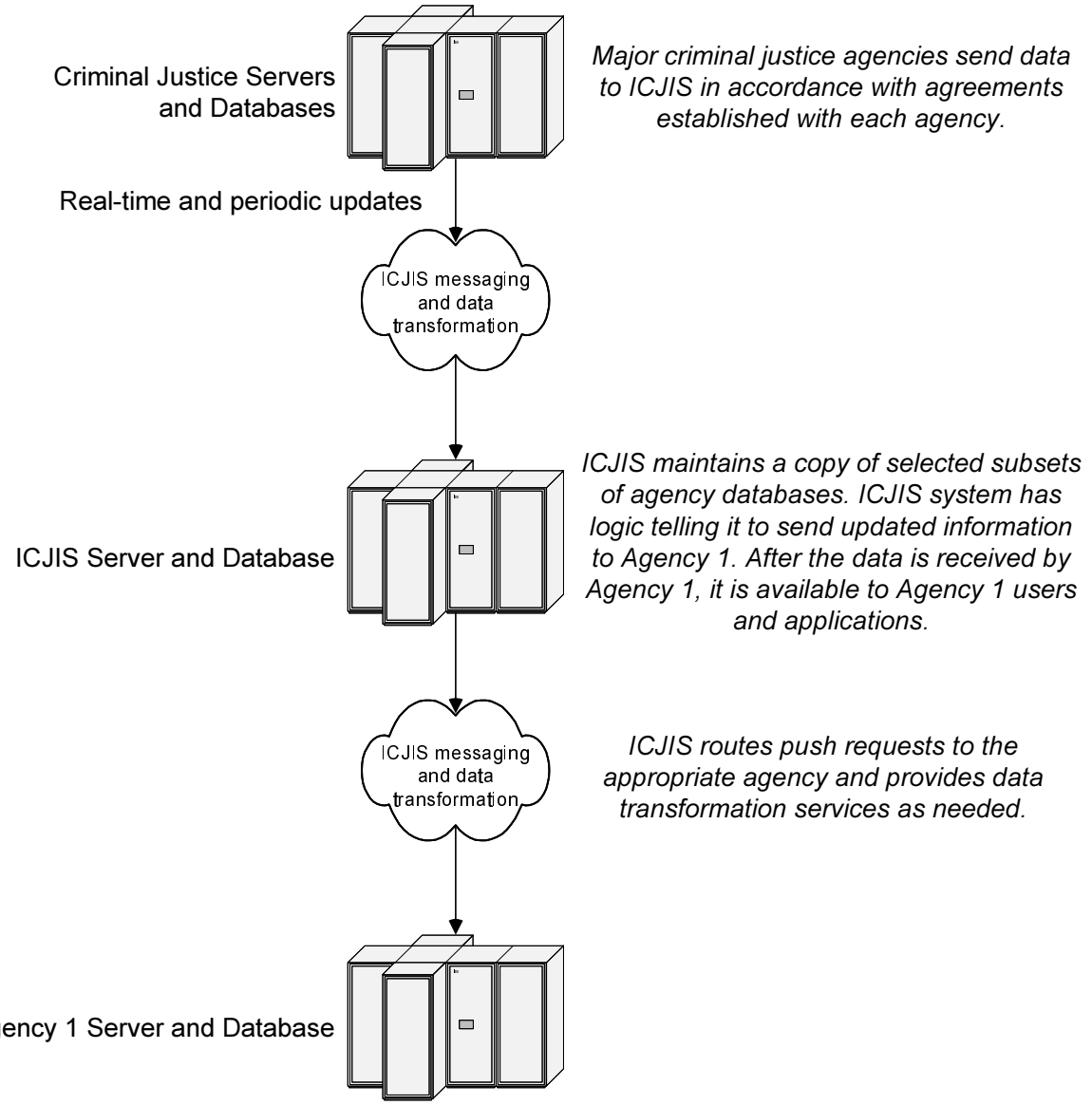

Figure 4.1.3-2. Push—Scenario Two: ICJIS to Agency

Figure 4.1.3-1 shows how an application running on a system in Agency 2, perhaps but not necessarily under the control of a local on-line user, determines that it has data that should be transmitted to one or more systems operated by other agencies. Conceptually, the data pushing scenario is the opposite of the data pulling scenario. Instead of the system needing data asking for it, the system that possesses the data takes the initiative and sends it to systems it knows will need it in the future. A data push is equivalent to one system asking another to update its databases with the new information being provided.

Once an application program determines that it should transmit data to a particular external system, it will generate one or more ICJIS standard transactions and pass them to an ICJIS interface module. The role of ICJIS will be to route the pushed data to the appropriate target system(s) and provide any data translation services that may be needed

between the systems. An application program on the target systems would accept the pushed data and take whatever action the receiving system deems appropriate. The general expectation is that the receiving system would store the pushed data, trigger some action (e.g., open a new case file), and/or alert an appropriate human user.

Depending on the implementation, the ICJIS *push* interfaces may be implemented entirely on the two cooperating agency hosts, or may involve a central ICJIS server that handles some of the processing on behalf of the agency host systems.

Figure 4.1.3-2 shows an alternate scenario where an application running on the central ICJIS server may push data to an agency system. In some cases, this may occur as a result of a database update or other action by an ICJIS user; in other cases, the receipt of updates to the ICJIS copies of agency databases may trigger processing logic that says another agency should be told about the update.

4.1.4 Inter-Agency Event Subscription and Notification

The ICJIS solution should allow an on-line user or agency application program to *subscribe* to an automatic notification service from another agency's application if and when a particular event occurs in the future. An example might be a probation officer requesting notification if a particular client is arrested for a crime.

Another example would be to provide more timely information about events occurring in the courts or commonwealth attorney offices to the victim notification system at the Department of Corrections. This would improve the accuracy and timeliness of required notifications to victims regarding an offender's status. In fact, given the desire and funding, ICJIS makes it possible to envision an integrated, statewide victim/witness notification system that tracks an accused or convicted offender from arrest and trial to conviction, incarceration, and release.

Figures 4.1.4-1 and 4.1.4-2 show scenarios for how the subscribe and notify functions might work.

Figure 4.1.4-1 shows how a user at Agency 1 would submit a subscription request for notification if a particular event occurs. The operational concept is that ICJIS would design some sort of standard interface that would allow a user to specify exactly what event he/she is interested in. The types of events supported would perhaps be selected from a list, with the user keying in additional parameters such as the ID of a person or case of interest.

ICJIS would translate and route the subscription request to the appropriate target system(s). The target system(s) would then be responsible for monitoring for the occurrence of the event, and providing notification if and when the event occurs.

Depending on the implementation, the ICJIS *subscribe* and *notify* interfaces may be implemented entirely on the two cooperating agency hosts, or may involve a central ICJIS server that handles some of the processing on behalf of the agency host systems. How the monitoring function is implemented may vary from system to system, and each system would be asked to monitor only the types of events it has agreed to monitor.

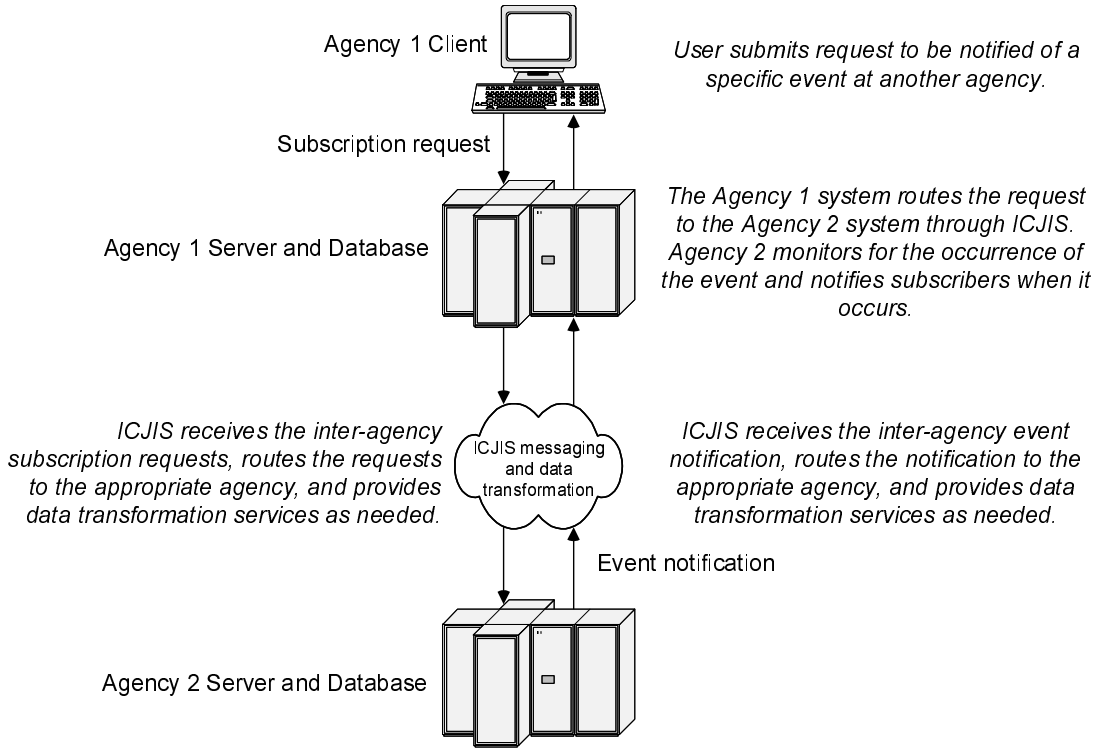

Figure 4.1.4-1. Subscribe/Notify—Scenario One: Agency to Agency

Figure 4.1.4-2 is an alternate scenario in which the central ICJIS server would provide subscription and notification services for its own databases, as well as on behalf of some agency systems. In this scenarios, subscriptions would be accepted by the central ICJIS server, and ICJIS would monitor for the occurrence of events of interest. Events would be detected either directly by ICJIS, or indirectly upon ICJIS receipt of periodic database updates from agency systems.

Whether events are monitored by ICJIS or by agency systems, notifications must be generated and routed to all subscribers when an event of interest occurs. From the viewpoint of the requesting user, such notifications will be received completely asynchronously; i.e., the event may occur the day after a subscription is submitted, a year later, or perhaps never. An individual user may submit many subscription requests over time. The method for presenting event notifications to the user should therefore include enough event-specific data to make it clear which event has occurred.

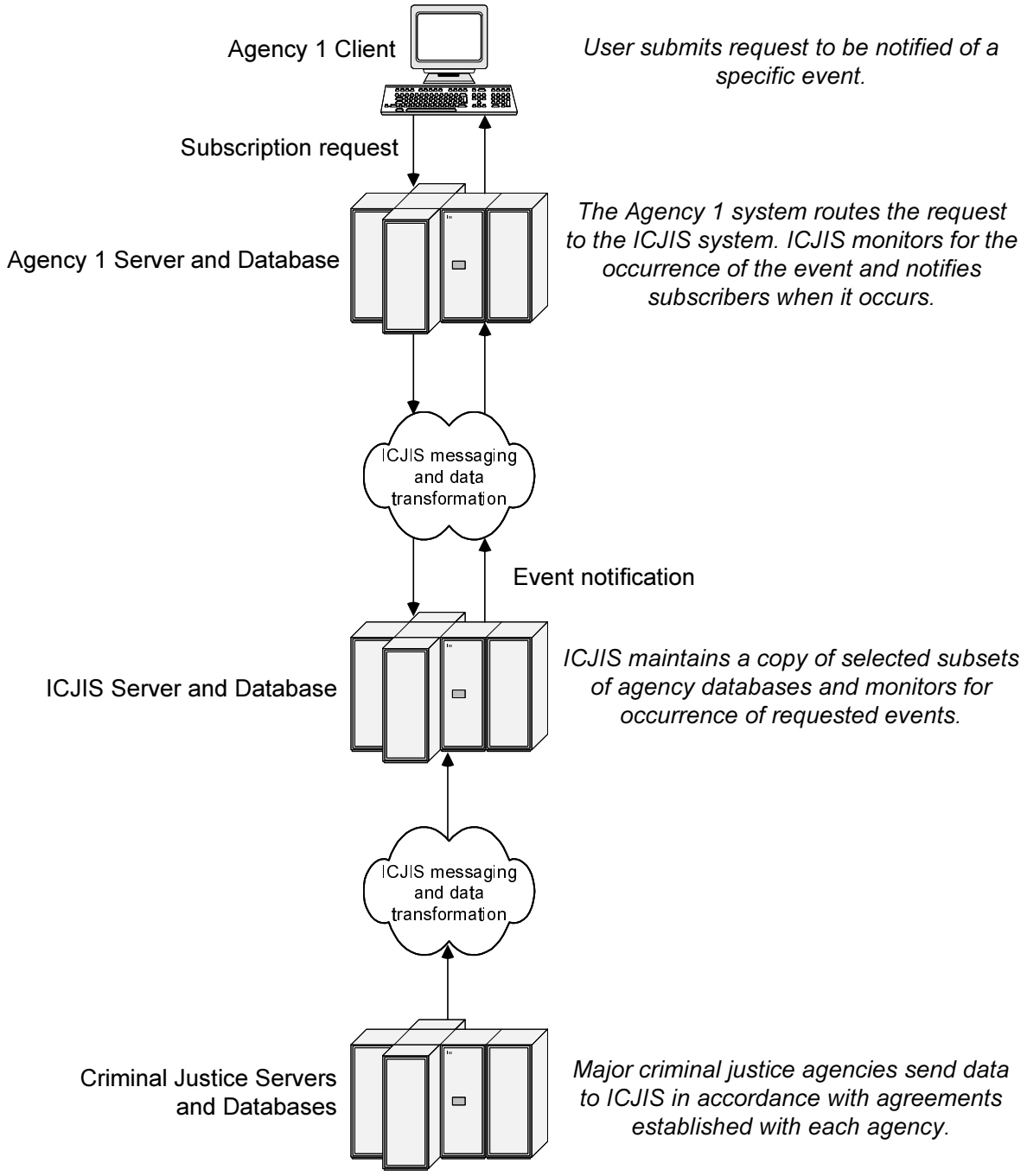

Figure 4.1.4-2. Subscribe/Notify—Scenario Two: Agency to ICJIS

4.1.5 Inter-Agency Information Publishing

The ICJIS solution should support a mechanism for any authorized agency to *publish* (i.e., post) announcements, reports, or other information of interest to the overall ICJIS community, so that it is accessible on-line by ICJIS users. Publishing is a useful way to disseminate information in a non-database-structured format to a wide audience. Examples might include policy guidelines, bulletins and announcements, reports, and court schedules. Figures 4.1.5-1 and 4.1.5-2 show scenarios for how this function might work.

As shown in Figure 4.1.5-1, the operational concept for this function is that ICJIS will maintain a hosting service for use by any agency that wishes to share information via on-line publication. Material to be published may be submitted by the ICJIS itself or by any of the participating agencies.

A well established and therefore a likely candidate approach is the use of web server and interface technology. ICJIS could maintain a web site on a central server, where agencies could post material directly, or post links to material on agency-specific sites.

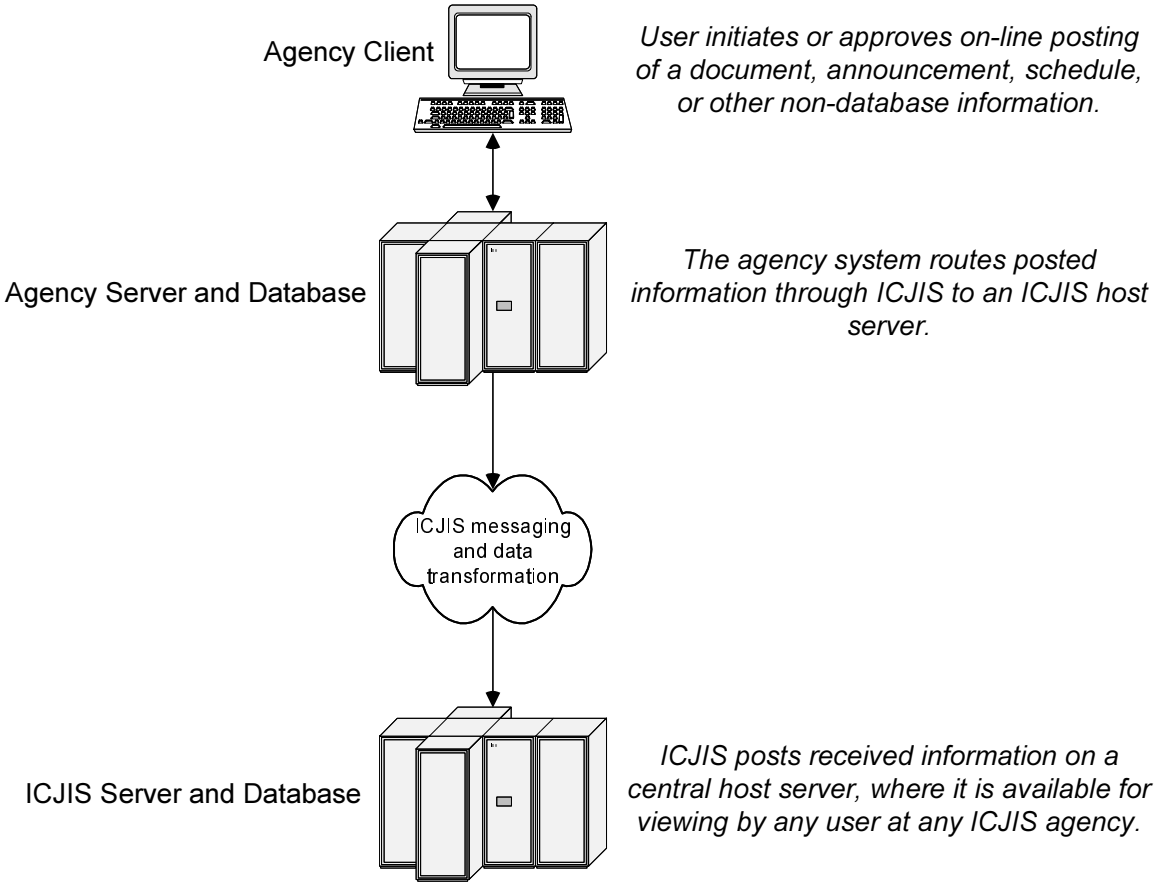

Figure 4.1.5-1. Publish—Scenario One: Posting of Published Information

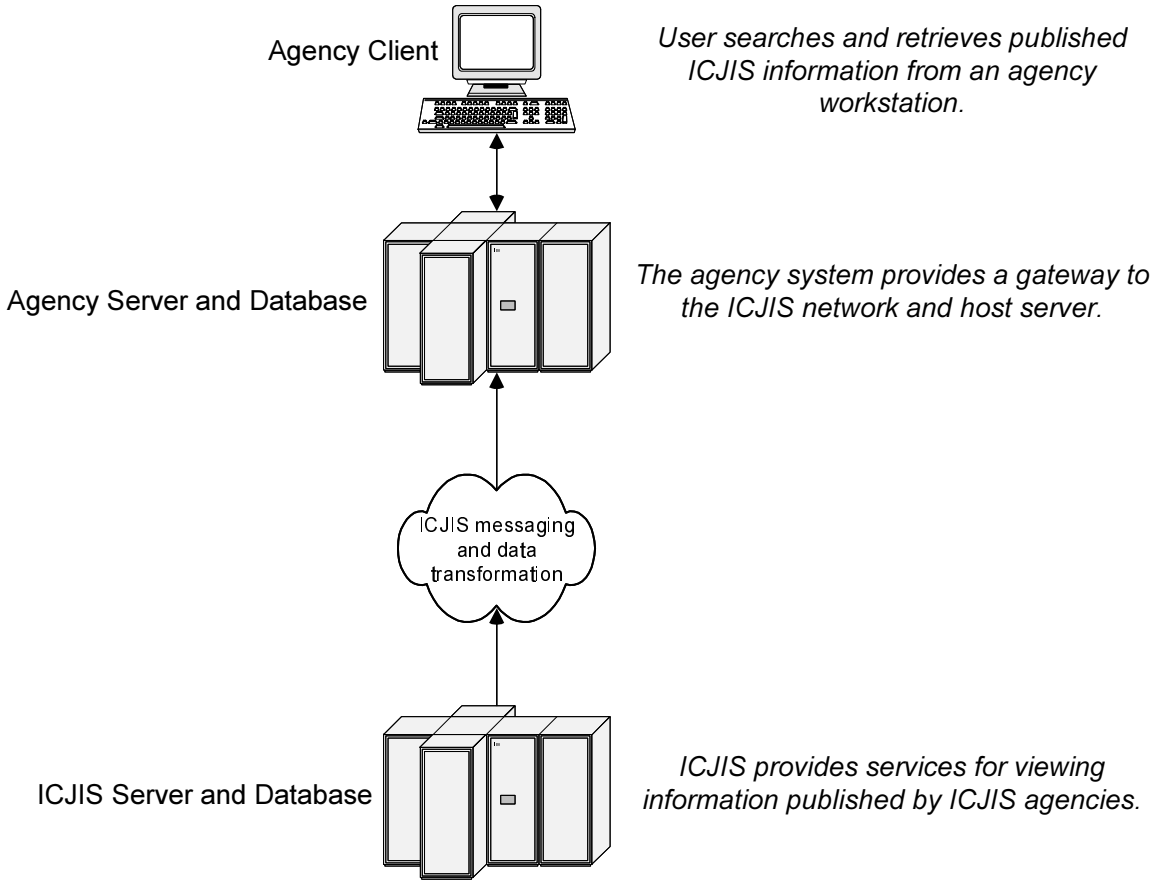

Figure 4.1.5-2. Publish—Scenario Two: Retrieval of Published Information

Figure 4.1.5-2 shows the scenario for accessing published information. Users would be able to browse the host site and bring up any posted information of interest. Although the diagram shows the user going through an agency host system to gain access to the central site, direct user access would also be possible, particularly if web technology is used.

The posting process should probably be a human-moderated process, wherein users submit items for inclusion that are then checked, approved, and published. The human moderator would also establish policies regarding currency—for example, deleting information after a fixed time unless the submitter either updates it or reasserts its currency.

4.1.6 Inter-Agency Aggregate Data Assembly and Analysis

The ICJIS solution should support tools and databases needed to perform trend and statistical analyses using combined historical data from participating database systems. Based on requirements and design analyses, the ICJIS program has determined that a data warehouse is the only architecture that will support potentially complex and resource-intensive data analyses without causing unacceptable impacts on operational agency systems.

As shown in Figure 4.1.6-1, the operational concept for this function is that ICJIS will create and maintain a data warehouse of

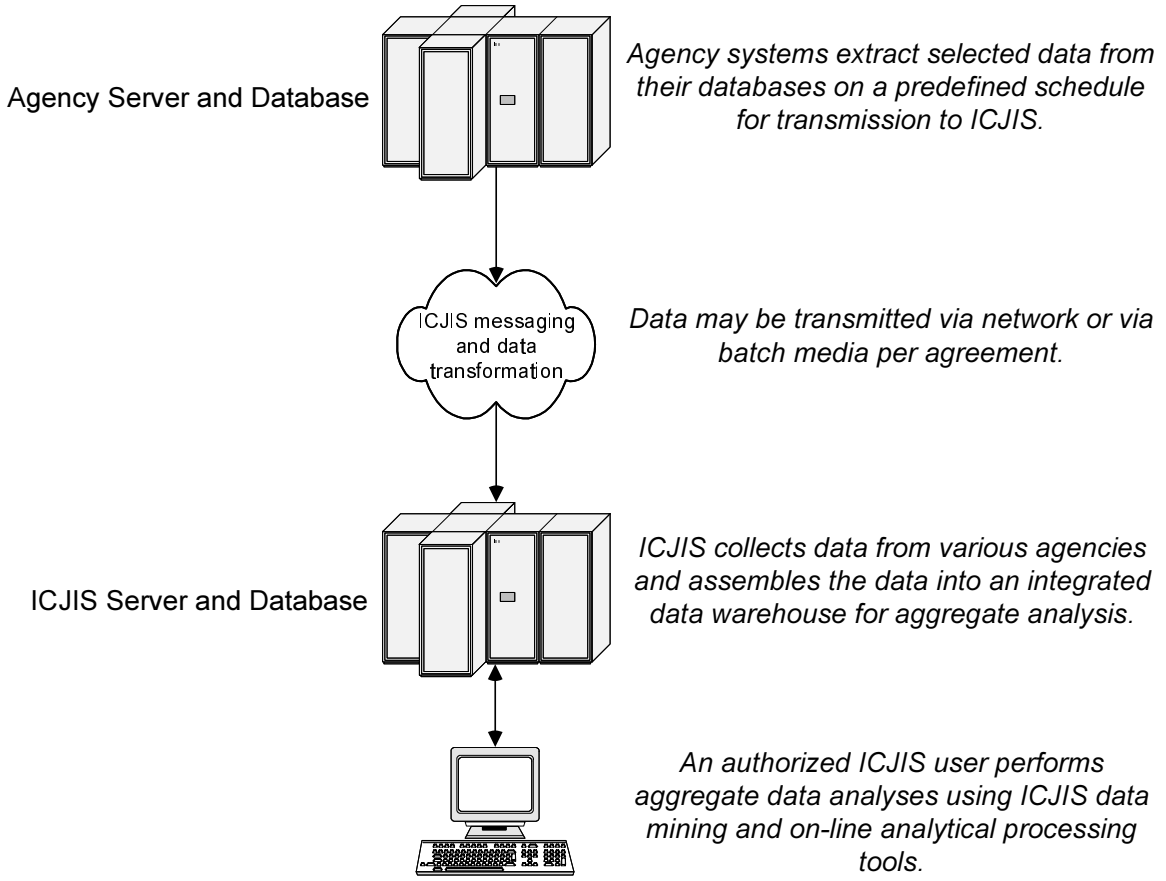

Figure 4.1.6-1. Aggregate Data Assembly and Analysis

relevant historical data extracted from participating agency databases. ICJIS will also provide authorized users with data mining and on-line analytical processing tools to help perform the desired analyses.

The data warehouse will be initially populated using data extracted from participating agency systems. Thereafter, the role of the agency systems will be limited to providing periodic data updates to the warehouse. The specific contents of the warehouse, tools to be provided, and frequency of data updates are all implementation decisions. It is likely that warehouse contents and capabilities will be allowed to grow gradually, rather than be implemented all at once.

4.2 Concept of Operations: Data Linking Functions

There is implicit in most of the six fundamental integrating functions (all except data publishing) a requirement that cooperating agency systems be able to share a common understanding of exactly what individual or event is being referred to by the data being shared. When data is being queried, pushed, pulled, subscribed to, notified, or assembled about a particular individual or case, there must be some way to uniquely identify the individual or case that all participating systems will understand.

As was discussed in Section 3.3.2 (the Data Standards and Linkage Problem), this can often be a serious problem in practice, due to

the fact that independently developed agency systems often use system-specific unique IDs to key their records. The key used to identify an individual or case in one agency system may be totally different from the key used at a different agency, or even in a different system within the same agency.

For this reason, the ICJIS operational concept should include mechanisms for identifying records in multiple agency databases that refer to the same individual or case. These mechanisms may be thought of as linking processes for individuals and cases

4.2.1 Inter-Agency Data Linking for Individuals

The ICJIS solution should provide mechanisms for identifying related and potentially related data on a particular individual from any of the participating database systems. Simply having access to multiple agency databases is not enough without the ability to tell when records do or do not refer to the same person.

This problem arises because the standard personal identification keys used in most civilian database systems (e.g., name and social security number) are not reliable when dealing with suspects and offenders. Criminals are often motivated to conceal, change, or misrepresent their true identities, personal records, and criminal histories. As a result, over a period of time, it is very possible that different agencies will have data about the same individual but under different identifiers. (It is also possible that different agencies will have data under common identifiers but which actually relate to two different individuals, due to one individual stealing or borrowing another's identity.)

The solution adopted by most criminal justice agencies to reliably identify an individual is based on fingerprint matching. In Virginia, the Virginia State Police provides fingerprint matching services for statewide law enforcement organizations. The VSP in turn has network access to FBI fingerprint matching services. When a fingerprint match is found, the VSP returns a State ID (SID) code unique to the matched individual. The SID may be used to retrieve criminal history information and any other records held by ICJIS agencies under that ID.

Unfortunately, there are often times when it is inappropriate or impractical to conduct a fingerprint ID check at point of initial data capture. As a result, many Virginia criminal justice databases track information about suspects and offenders on keys that are computer-generated and therefore unique to each database. These system-specific keys are totally meaningless to other criminal justice systems and to human users who may be interested in retrieving information about an individual.

To address this problem, the operational concept postulates the existence of biographic ID matching services on the ICJIS network. Such services would link data at different agencies based on matching various combinations of identifiers other than fingerprints. These might include name, address, social security number, date of birth, physical characteristics, distinguishing marks and scars, DNA, etc.

As shown in Figure 4.2.1-1, ICJIS anticipates that such linking services would be provided on a central ICJIS server. There are three basic reasons for this approach:

- Linking by definition requires that data be retrieved and compared from multiple agency databases. It makes sense to bring the data together on a central server rather than on a particular agency system.

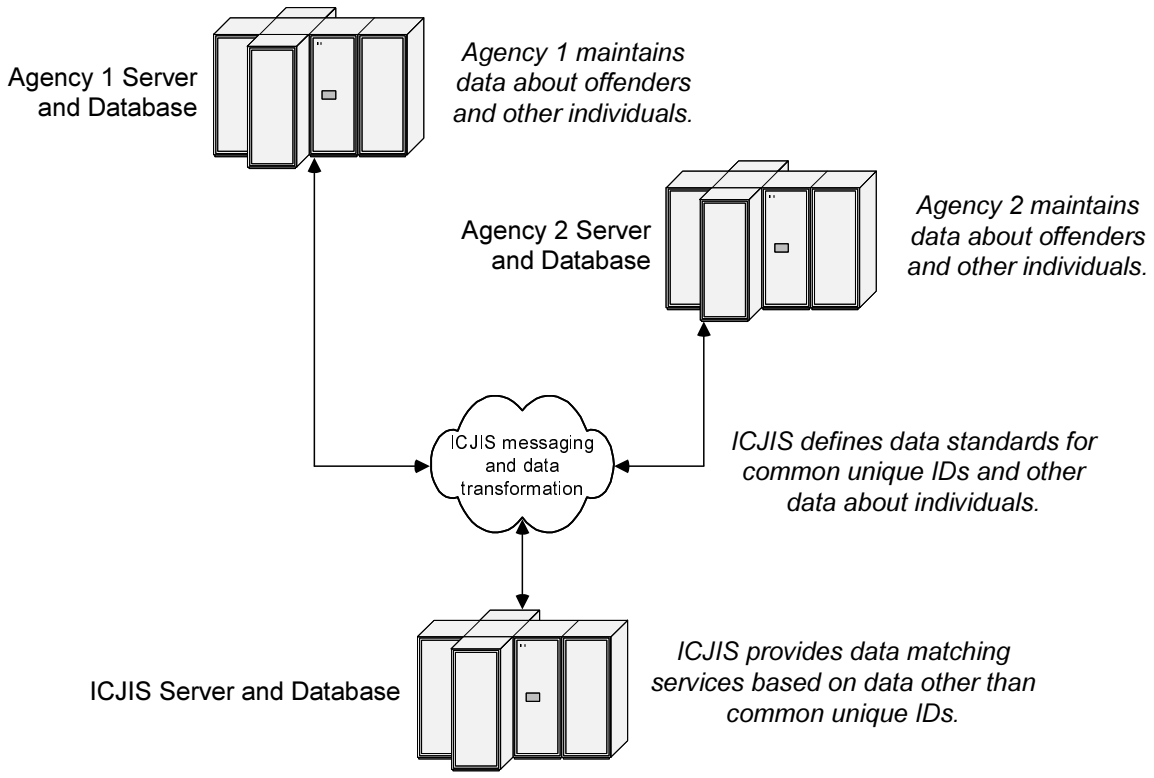

Figure 4.2.1-1. Inter-Agency Data Linking for Individuals

- Linking algorithms may require significant processing time and resources. Linking is envisioned as a heuristic process based on a collection of algorithms. For example, some algorithms may make decisions based on approximate name matching and statistical techniques such as Bayesian inferencing.
- Once identified, links and candidate links should be stored in a central database long term. This will allow subsequent users to make use of the links, or to further validate them.

Because linking will potentially be a lengthy activity, the user should not be forced to wait for the results before going on to another activity. The user should be notified in some way when the link results are available.

4.2.2 Inter-Agency Data Linking for Cases

The ICJIS solution should provide mechanisms for identifying data related to a particular offense or case from any of the participating database systems. Conceptually, this function is similar to the linking of data about individuals. In practice, the problem is significantly less complex because case identifiers are not subject to concealment or falsification by criminal offenders.

Under ideal circumstances, whichever agency *officially* opens a case should have a facility for assigning a unique ID to that case and then sharing that ID with all other agencies that may later become involved. Each agency in turn would have mechanisms for accepting the unique ID, tying all case records to that ID, and passing

the ID along to other agencies who may need it.

In practice, there is currently no enterprise-wide mechanism for assigning a common unique charge or case ID.

To address this problem, DCJS, the Supreme Court of Virginia, the Virginia State Police, and other agencies have organized the Charge Standardization Project to design and develop system functionality that will assign standardized charge numbers to all new charges. These numbers will be shared with other agencies that need access to charging information from other agencies.

Please see the business case for the Charge Standardization Project for additional information.

4.3 Mapping of Functions to Business Problems

Figure 4.3-1 relates the eight information system functions described in this section to the five major business problem areas discussed in Section 3. As can be seen, each of the functions directly addresses one or more business problems, and each business problem is addressed by one or more functions.

ICJIS Function	Business Problem(s) Addressed
Inter-Agency On-Line Query	Addresses Data Accessibility problem by providing authorized users with on-line network access to relevant data from all participating agency systems.
Inter-Agency Information Pulling	Addresses Data Accessibility problem by providing authorized application programs with network access to data from other agency systems. Addresses Data Quality problem by reducing redundant manual data entry, thereby reducing opportunities for errors, omissions, and inconsistencies. Addresses Inter-Agency Coordination problem by automating the process of requesting and retrieving relevant data from other agencies.
Inter-Agency Information Pushing	Addresses Inter-Agency Coordination problem by allowing one agency to automatically transmit information to another agency that will need it, thereby eliminating delays and oversights in the hand-off of a case from one agency to another. Addresses Data Quality problem by reducing need for redundant manual data entry by receiving agencies.
Inter-Agency Event Subscription and Notification	Addresses Inter-Agency Coordination problem by allowing a user to request automatic notification if an event of interest occurs at another agency, and by allowing a system to deliver automatic notification to a list of subscribers if an event occurs that is of interest to users at other agencies. Automation of this service reduces delays, oversights, and uncertainties in sharing information about critical events of interest among multiple agencies.
Inter-Agency Information Publishing	Addresses the Data Accessibility problem by giving authorized users on-line access to useful reports, announcements, and other information posted by other agencies.

ICJIS Function	Business Problem(s) Addressed
Inter-Agency Aggregate Data Assembly and Analysis	Addresses the Aggregate Analysis problem, thereby enabling authorized policy analysts and researchers to perform a wide range of useful studies and analyses.
Inter-Agency Data Linking for Individuals	Addresses Data Standards and Linkage problem by providing mechanisms for identifying and linking data from multiple systems that relate to the same individual, when no common unique ID is available.
Inter-Agency Data Linking for Cases	Addresses Data Standards and Linkage problem by providing mechanisms for identifying and linking data from multiple systems that relate to the same charge or case.

Figure 4.3-1. Mapping of ICJIS Functions to Business Problems

5. Recommended System Architecture

Section Overview

Purpose: To describe a general system architecture for implementation of the ICJIS concept, and to briefly discuss major architecture issues and trade-offs being investigated by the ICJIS program.

Key Points:

- The ICJIS program's approach to system architecture is based on recognition of the fact that the Virginia criminal justice community is already supported by many very capable information systems, so there is no need to start from scratch.
- The ICJIS approach to system architecture also places high priority on minimizing potentially disruptive impacts on operational agency systems.
- The recommended ICJIS system should be viewed as a "system of systems," linking together many cooperating but independent agency systems, rather than as a large monolithic centralized system in its own right.
- The ICJIS architecture includes the following major infrastructure components: a wide area network, ICJIS gateway interfaces added to cooperating agency systems, new and/or modified user interfaces, and one or more central ICJIS server(s).
- The ICJIS program is investigating issues and trade-offs in several major aspects of the architecture, including but not limited to: the location of databases on the network, data standards and translation services, network message format standards, network security and data privacy, application programming interfaces, and integration with the VCIN network.

The ICJIS approach to system architecture is based on the fundamental premise that we are not starting from scratch. The Virginia criminal justice community has built up an extensive legacy of effective business processes and information systems that are woven into the day-to-day operations of the agencies and people they support. To achieve the ICJIS vision cost effectively, it would be unnecessary, and unwise, to require wholesale replacement of these existing processes and systems with something entirely new.

In evaluating potential ICJIS system architectures, DCJS has given high priority to minimizing the changes needed on existing systems. This objective will be largely met but, in some cases, more extensive changes will be needed. For example, new charging information is needed from magistrates, but the existing system's design does not allow this information to be shared efficiently. Through the Charge Standardization Project, alternative designs are being evaluated to address integration requirements.

Some agencies are already interested in reengineering their systems to meet internal needs. This provides an ideal opportunity to incorporate ICJIS integration functions into their new systems. But where desire for changes to a particular system does not currently exist, the ICJIS program will make every effort to minimize changes needed to accommodate integration.

5.1 Components of the Architecture

In our approach, the ICJIS system should be conceptualized as a network of cooperating but independent agency-controlled information systems. By agreeing to participate in ICJIS, an agency system commits to support certain well defined, mutually agreed, interactions with other systems. But each system retains its individual autonomy and control over its own operations, and each system's primary responsibility will continue to be to provide mission support to its own community of users.

In this way, ICJIS may be thought of as a loosely coupled "system of systems" rather than a monolithic system in the traditional sense. This "system of systems" architecture is illustrated in Figure 5.1-1. The diagram is intended to show the major conceptual components of the architecture, rather than a specific implementation. Each of the major architectural components is briefly described in the subsections below.

5.1.1 The ICJIS Network

In order to implement the integrating functions described in Section 4, each participating system must have data communications paths available to talk to every other system with which it wishes to exchange data. In addition, there must be data communications paths linking the systems to a potentially very large and geographically dispersed user community.

The ICJIS concept therefore requires some sort of backbone wide area network (WAN) capable of connecting criminal justice

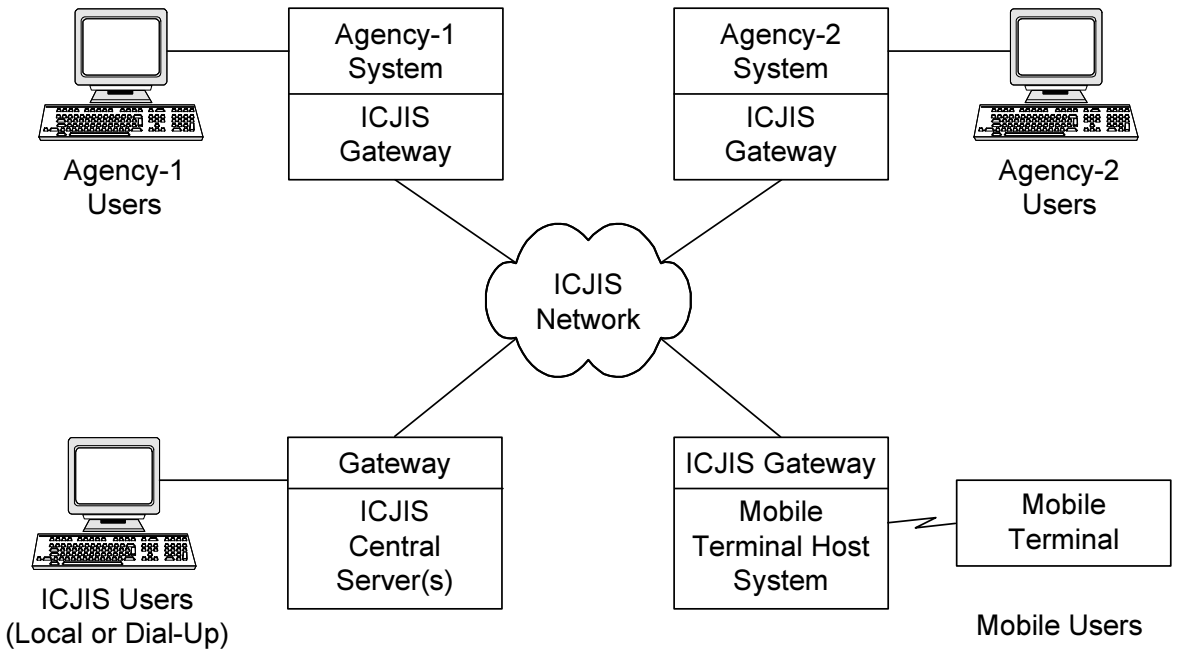

Figure 5.1-1. The ICJIS Architecture will be a "System of Systems"

systems and users throughout the state. In Figure 5.1-1, and throughout this document, this network is referred to as "the ICJIS Network."

This should not be taken to mean that ICJIS proposes to construct a new dedicated network from scratch. The preferred approach would be to piggyback on an already established statewide government or law enforcement network to which all ICJIS systems and users could be given access. If there were isolated offices where access to the preferred network is not available, dedicated WAN connections (e.g., frame relay circuits) could be installed from the office to an ICJIS central server, thereby providing access to the rest of the ICJIS network.

A second option would be to support dial-up connections to an ICJIS central server acting as a network hub. This option could be cost-effective for small agencies and individual users with a need for only intermittent access to ICJIS. Another even lower-cost alternative would be to use a public network such as the Internet, although this may be less desirable due to security and privacy considerations.

Due to the diversity and geographic dispersion of potential ICJIS users, some hybrid or combination network architecture may prove to be most cost-effective. As part of ongoing planning activities, DCJS is evaluating network alternatives in order to arrive at a design recommendation.

5.1.2 Agency System ICJIS Gateways

As indicated in Figure 5.1-1, the ICJIS architecture requires that each cooperating system install some sort of gateway between itself and the ICJIS network. Conceptually, the gateway is the complete set of hardware and software components needed by a particular system to interface with the network and to process all agreed-upon ICJIS transactions.

In practice, the scope and physical implementation of this gateway may vary widely from system to system. For example, from a hardware perspective, some systems may choose to install a new processor to serve as an ICJIS front end to their main information system(s). Other systems may choose to implement ICJIS gateway functions on existing computing platforms.

From a software perspective, different systems may choose to implement different mixes of ICJIS functions. For example, some systems may choose to support subscription and notification services to external users, while other systems may not. The manner of implementation of common functions may also vary to reflect differences in computing platforms, DBMSs, and programming languages. To maximize commonality and minimize software development complexity, DCJS recommends that common commercial off the shelf packages and application programming interfaces (APIs) be used whenever possible (see Section 5.2.5).

In many cases, agency systems already possess some of the hardware and software interfaces needed to support ICJIS functions. Many systems are already network capable, and some have interface software supporting remote access to their databases. Where new gateway functionality must be implemented, risk is reduced by the fact that core ICJIS interfaces may be implemented largely, although not entirely, using commercially available software. As part of ongoing planning activities, DCJS is evaluating key agency systems to determine what upgrades would be required to make them fully capable of supporting ICJIS functions.

5.1.3 User Platforms and Interfaces

As indicated in Figure 5.1-1, the ICJIS architecture anticipates that several different types of user platforms and connectivity paths may have to be supported. The three general categories of user platforms are:

- Users on workstations who are connected to an agency mainframe or local area network which in turn provides the user a gateway to the ICJIS network
- Users with personal desktop computers who link directly to the ICJIS network via dial-up connection
- Users with mobile data terminals or other wireless interface equipment

ICJIS is intended for a broad spectrum of users. Some will be law enforcement or criminal justice personnel employed by state government departments. Others will be affiliated with local governments or the federal government. Given the diversity and wide geographic dispersal of the potential user population, it is vital that ICJIS provide a user interface that is easy to deploy and maintain.

One option ICJIS rejected from the start is use of special purpose workstations for ICJIS user functions. Such an approach, aside from being very expensive, would cause office space and desk space problems for ICJIS users, who in most cases already have a PC or other workstation in their work area and do not have room for another.

The decision was made to make the default ICJIS user interface compatible with workstations already being used by the ICJIS user community. For the vast majority of users, this means standard Windows-based PCs.

Given this environment, ICJIS is recommending that the default user interface be built using web browser technology. A web-based user interface is inherently self deploying, is familiar to almost all users, and is good at combining text, images, and relationships such as references or information drill-down. Web interfaces are associated with the HTTPS secure network protocol that can provide mutual authentication of user and server, confidentiality, and data integrity protection.

Web interfaces are not as subtle as custom built graphical user interfaces such as native Windows interfaces. If additional user interface capabilities are needed, web-based interfaces can be extended using Java, or another browser compatible programming language, without losing any of their benefits.

Some tailoring of the default user interface will be required to support users with Mobile Data Terminals (MDTs) or handheld wireless devices. Such devices have limitations in the areas of communications bandwidth and web displays that may require limiting the ICJIS capabilities available in a wireless setting.

5.1.4 ICJIS Server(s)

As shown in Figure 5.1-1, the recommended system architecture includes a component called the ICJIS Server(s). This is envisioned as a relatively modest suite of computing equipment maintained at some logically central location.

In theory, any of the functions allocated to the ICJIS servers could also be allocated to one or more agency systems. However, there are several ICJIS functions that would benefit from the existence of dedicated ICJIS central servers, independent of any existing agency system. These functions, discussed below, have fundamental multi-

agency scope, and thus do not naturally fit within the statutory purview of any one agency.

- The information publishing function will likely be implemented in the form of web pages or web links to on-line documents. It makes sense that a shared ICJIS web site be maintained on a central ICJIS server.
- The aggregate data assembly and analysis function requires that a data warehouse be created and maintained from data extracted from many different agency databases, and that a suite of specialized data mining and on-line analytical processing tools be provided. It makes sense that the data warehouse and aggregate analysis tools be maintained on a central ICJIS server.
- The inter-agency linking functions for data about individuals and cases by definition requires extracting and comparing data from multiple agency databases. In addition, some linking algorithms would require retrieval of data based on non-key fields, causing potentially major impacts on database system performance. It is also likely that a central database of identified links and suspected links would be useful to ICJIS users. For all these reasons, it makes sense to implement the linking functions on a central ICJIS server.
- As was discussed in Section 4, there is a possibility that several other major integrating functions will be partially implemented on a central server rather than fully distributed to agency systems. Examples include having a central server maintain and process subscription lists on behalf of notifying agencies, or using a central server to queue pushed data when the target agency system is not available to receive it. The general idea is to use the central server as needed to make life easier for the agency systems.
- As was discussed in Section 5.1.1, a central server is a logical place to provide dial-up ports or other network interfaces for small agencies and individual users not otherwise connected to the ICJIS WAN.
- As was discussed in Section 5.1.3, the default user interface for on-line ICJIS functions will be web browser based. It makes sense that the content of this interface (i.e., the web pages and associated processing logic) be maintained at one central server, rather than be replicated at every agency.
- As will be discussed in Section 5.2.1, there is a possibility that some portions of agency databases may be replicated and maintained on a central ICJIS server, in order to reduce or eliminate potentially disruptive external accesses to those agency databases.
- There will be a system management and administration component to maintenance and operation of the ICJIS after deployment. There will be a need for some amount of software update, testing, configuration management and the like. It makes sense that such functions be performed on a central ICJIS server before deployment of changes to statewide user platforms.

The ultimate physical and organizational location of these central servers is an open question at this point. DCJS will be managing ICJIS development, so it is likely that the central ICJIS servers will be located at DCJS during the development phase. However, DCJS does not view creation and maintenance of a significant IT organization as part of its mission. The management of the ICJIS central servers may therefore be

transferred to another organization after development. A decision on this issue will be part of the program's long-range planning process.

5.2 Architectural Design Issues and Trade-Offs

Within the general framework of the conceptual system architecture described above, there are many detailed design issues and alternatives for implementation. As part of ongoing planning and requirements analysis activities, DCJS is analyzing design alternatives and trade-offs, and will work with stakeholder agencies to cooperatively arrive at cost-effective design decisions.

The following subsections briefly discuss the major architectural issues and alternatives under consideration. Although some of this material may be somewhat technical for purposes of a Business Case, it is included here to give decision-makers some perspective on the scope of the technical challenges being addressed by the ICJIS program.

5.2.1 Location of Databases on the Network

One of the fundamental architectural issues facing ICJIS designers is the physical location of ICJIS databases. It is a given that multiple agencies currently own portions of the overall ICJIS data store. These agencies have a statutory responsibility to collect and maintain certain data, and to make that data available to authorized users in performance of their missions. Integration with ICJIS will not relieve the agencies from these responsibilities.

From the agencies' point of view, integration with ICJIS opens up their database systems to a potentially very large new community of users. This prospect has raised some concerns about potential performance impacts on agency systems, potential exposure to security and privacy threats, and potential loss of control over data needed for agency-specific purposes.

Given these concerns, ICJIS has analyzed three basic choices relating to data location.

1. ICJIS users could retrieve data directly from the agency systems via ICJIS network access, with carefully designed and agreed-on procedures for protecting agency systems from adverse performance and security impacts.
2. ICJIS could maintain a copy of selected agency data on an ICJIS central server, so that most (if not all) retrieval requests would be handled by ICJIS rather than by agency systems.
3. Some primary agency databases could be relocated to a powerful central ICJIS server, capable of supporting all performance and security requirements, with agencies maintaining their data remotely via network database access.

Option #1 is the approach that the ICJIS program has prototyped in the early stages of requirements analysis. It is logistically the least complex of the three options, as it entails no changes to the way agencies currently maintain their databases. Integration with ICJIS in effect merely adds to the number of users and programs accessing those databases. Design solutions are available for limiting the number of simultaneous hits a database may take from external ICJIS users, and for upgrading security controls. Nevertheless, where there are legitimate performance and/or security concerns, ICJIS will consider alternatives to direct agency system access.

Option #2 makes the ICJIS in effect a proxy server for agency database systems. The scenario would be that each agency would

extract only those portions of its databases that it is willing to share, and send it to ICJIS, which would load the data into database(s) on an ICJIS server. All outside agencies and users would then be allowed to query the ICJIS copy of the agency databases, but would not be permitted to access the primary agency databases directly.

Besides eliminating outside access to operational agency databases, this approach has the benefit of faster response times for ICJIS queries. DCJS requirements analyses have indicated that, with the exception of databases at the Virginia State Police and the Supreme Court of Virginia, ICJIS users will actually need access to a relatively small amount of the data contained in complex agency databases. In some cases, it may turn out to be more efficient and cost-effective to extract and copy the small amount of desired data rather than implement direct access to the entire database.

Section 4.1.1 summarizes other important benefits of using a centralized ICJIS database.

The obvious drawback to this approach is that the data in the extracted database may not be the most current data available. Each agency that owns data to be shared with other agencies would need to update the central ICJIS database. Depending on the agreements and technical solutions implemented, the ICJIS database could be out of synch with the agency's database by several seconds or several days. If updates are made on a frequent basis (e.g., real-time), this increases the processing requirements on the agency's system.

Despite these drawbacks, option #2 appears to be viable for some purposes given the anticipated benefits. Specific solutions should be explored with the major agencies that would contribute data.

Option #3 makes the ICJIS in effect a remote database server for multiple agencies. The scenario would be that selected operational databases would be physically relocated from their current agency computing platforms to one or more central ICJIS servers. Each agency would continue to be responsible for maintaining its own data, but would direct its I/O operations to an ICJIS server rather than an internal system. Outside agencies and users would then be able to access the data from the ICJIS server, eliminating any contact with the source agency's internal systems.

This option has many operational drawbacks. Depending on the operating systems, programming languages, and databases involved at a particular agency, it probably implies significant changes to agency applications, and an extremely high level of inter-agency cooperation that is not practical for many reasons (e.g., certain loss of control of agency data). In addition, the central database site would need to be powerful enough to handle the total user database management load across all agencies, operate on a 24x7 schedule, and have complete redundancy. Many agency systems are already staffed and operated at on a 24x7 basis. These personnel and other resources such as backup power generators may need to be relocated or (more likely) duplicated.

Based on these preliminary analyses, ICJIS has eliminated option #3 but is considering a possible hybrid of options #1 and #2. It may be feasible to use an ICJIS copy of some agency data to support some integration functions, while using direct access to agency databases to support others. As part of ongoing planning activities, DCJS is continuing to evaluate these options to

determine which approach makes the most sense on a case by case basis.

5.2.2 Data Standards and Translation Services

Another fundamental design issue is how to handle the problem of *semantic heterogeneity* across agency databases. This refers to the fact that the same type of information may be stored on different agency systems using different data formats, coding systems, units of measure, and the like.

A simple example is a person's name. An ICJIS user may want to search multiple agency databases for records on a criminal suspect. The problem is that one system may store a person's name in the format <last name, first name> in a single field, while another system may store the first and last names in separate fields.

Another example might be a person's height. One system may store height as feet and inches, while another may convert to total inches. Still another example might be a field such as race or hair color. In some systems, such data may be stored in plain text, while in others the data may be encoded as numbers corresponding to a list of valid entries.

The point is that when a user sets out to query multiple agency databases, he/she must be aware of these differences and compose the query accordingly. Similarly, when one system pushes or pulls data to/ from another system, the two systems must be able to understand each other's formats and coding systems to make sense of the data being exchanged.

In order to avoid forcing every ICJIS user and every agency system to be knowledgeable about every other system's internal data formats, the ICJIS proposes to implement translation services on behalf of ICJIS users and systems.

The ICJIS program is in the process of compiling an enterprise-wide data dictionary, documenting data items that are maintained in multiple agency databases. For each such data item, ICJIS will define an enterprise-wide standard format. This standard format will then be used to refer to that data item in all ICJIS queries and other transactions. The ICJIS would provide any necessary translations to and from the standard to system-specific formats.

DCJS has prototyped one possible implementation of this concept using a commercial product called IDS Integration Server (recently renamed Callixa). The system performance of the prototype was less than ideal, but the basic concept proved viable. Callixa reports that they have made substantial strides in performance levels over the past year, and there are now other products with similar capabilities. DCJS will continue to evaluate these products as potential solutions to the semantic heterogeneity problem.

Over the long run, of course, the intent is that agencies will gradually modify or upgrade their systems to adopt the standard formats, so that translation becomes no longer necessary. Realistically, this process will take many years, making translation services a mandatory part of the ICJIS design.

5.2.3 Network Message Format Standards

The integrating functions defined in Section 4 will likely be implemented as transaction messages between cooperating computer systems. In order for the systems on both sides of the transaction to understand each other, agreement must be reached on message format standards.

There are several good alternatives on which to base ICJIS message format standards. One approach would be to build upon a commercial messaging product (such as IBM's MQSeries) compatible with Virginia agency systems and relevant industry standards. ICJIS could then propose a solution specifically geared towards maximizing the efficiencies of data exchanges among Virginia criminal justice agency systems.

A messaging standard could also be based on newly emerging Extensible Markup Language (XML) standards. XML has been designed by an international standards committee to be a highly open and flexible meta-language for communication between disparate systems.

Within the criminal justice community, the National Law Enforcement Telecommunications System (NLETS) is in the process of implementing an XML-based rap sheet standard, which will eventually replace the existing ANSI/NIST standard. There is also a Legal XML group that is defining XML-based standards for other criminal justice transactions.

Use of XML would allow ICJIS to leverage a large and growing set of open source software tools. Also, newly emerging electronic document solutions, which are an important consideration in a legal environment, are usually based on XML.

The use of XML raises several issues, however. Mainframe implementations may require additional front-end hardware and software to be added to agency systems. XML is verbose (by design) and may cause significant processing overhead for some types of transactions. Based on current technologies, XML is not appropriate for real-time database queries. Queries should be based on ODBC or native database protocols.

Whatever formats are used, messages will need to be carried within a standard communications protocol such as SMTP, HTTP, FTP, SOAP, etc. At the transport layer, TCP/IP will be used.

Due to the asynchronous nature of some ICJIS integrating functions, one protocol worthy of strong consideration is the Simple Mail Transfer Protocol (SMTP). Although designed for use with electronic mail delivery, SMTP may be very applicable to ICJIS functions such as event notifications and data pushing. Notifications and pushed data are, like e-mail, received asynchronously from the viewpoint of the receiver, and SMTP is designed specifically to handle asynchronous deliveries. SMTP also supports storing messages and retrying transmission until the message is successfully delivered.

The best solution may be a combination of the protocols and message formats discussed above. For example, it might make sense to implement a commercial product-based solution for agency to agency messaging, an XML approach for electronic document management, and SMTP for notifications.

5.2.4 Network Security and Data Privacy

Security and privacy controls are vital for ICJIS because of the nature of ICJIS data. Some information is a matter of public record but access to other information is governed by privacy laws. Access must therefore be controlled and the data must be protected in transit over the network. Security and privacy impact assessments will be incorporated into the ICJIS system engineering and design methodology whenever potentially sensitive data are involved.

One major component of network security is user authentication. The primary connection

between ICJIS users and the ICJIS network is anticipated to be via the Secure Sockets Layer (SSL) to a web-based user interface on an ICJIS central server. Modern web interface technology includes strong security features. For example, this interface may include X.509 digital certificates for an added level of authentication. Even without client certificates, however, servers are authenticated to users (via server digital certificates), transmissions between user and servers are encrypted for confidentiality, and are protected via digests to guarantee integrity of transmission content. The ICJIS central servers could also perform application level logging of user access for security audit purposes.

If security controls are needed between ICJIS central servers and agency database systems, it is recommended that Virtual Private Networking (VPN) hardware be installed. This provides end-to-end encryption and server-to-server authentication using X.509 digital certificates. VPNs are transparent to software applications and hence do not affect the design or operation of any commercial or developed software.

ICJIS is aware that the Commonwealth is pursuing implementation of a Public Key Infrastructure (PKI) that would be the basis for providing authentication and confidentiality across all levels of government and users of ICJIS. PKI in the current commercial environment generally means use of X.509 digital certificates as the basis for secure authentication. These certificates are associated with web technology and the Secure Sockets Layer (SSL) because they were first widely used there but the potential use is broader. The Lightweight Directory Access Protocol (LDAP) is also associated with these elements but again is not actually tied to this use.

The use of digital certificates provides authentication and the secure distribution of a user or server's public key. Organizations that issue the certificates are called Certificate Authorities (CAs). CAs are typically commercial entities such as Verisign but any organization can become a CA. Web browsers are distributed with the public keys of the commercial CAs pre-loaded. If a user's digital certificate were issued by an authority unknown to the browser, verification could not be completely automatic. The use of a Commonwealth-wide CA might require or suggest a specialized version of the web browser with the Commonwealth's CA public key pre-installed along with other commercial CA keys.

5.2.5 Application Programming Interfaces

To facilitate standardized implementation of ICJIS functions, as well as to minimize software development costs, the ICJIS program plans to design and implement common APIs (Application Programming Interfaces) that will work in all agency environments.

An API is essentially a library of software services that perform detailed, low-level data processing functions on behalf of application programs. By developing an API for common ICJIS data processing functions, the ICJIS program would allow agency application programmers to focus on high-level business logic, and relieve them from having to deal with the details of ICJIS communications and transaction processing requirements.

Implementations of an API typically consist of software libraries that are linked to application software. APIs often consist of two parts—a client portion that is directly linked with client applications and a server

portion that implements the requested operation. There is often a network connection between client and server portions.

In the ICJIS setting, applications using a specific API may reside on a central ICJIS server and/or on multiple agency systems. This means that the APIs that are developed, particularly the client portions, may have to operate in more than one software environment. For example, the Virginia State Police has a Unisys 2200 series mainframe that is a likely candidate for developing an ICJIS application or a portion of one. The Supreme Court of Virginia, another likely candidate for developing an ICJIS application, operates a VM/VSE environment that is very different from the state police environment.

To address these realities, it may be necessary to implement the same ICJIS APIs in multiple environments. This may involve different programming languages such as C, COBOL, assembler, etc., as well as different sets of underlying operating system services including Unix (possibly several versions including Solaris and AIX), Windows NT, VM/VSE, Exec 2200, and MVS.

One possible approach is to build an implementation first using a standard programming language that operates across essentially all machines and operating environments, such as Java. A standard version of an API would be useful as a reference for development and testing of a preferred native implementation (in C or COBOL, for example) for a specific programming environment.

The scope of API development would be significantly reduced if a commercial package could be found providing some of the multi-platform API functions needed to implement ICJIS. DCJS is investigating candidate products such as IBM MQSeries.

5.2.6 Integration with VCIN

Several information systems that are key to the ICJIS concept are currently accessible through the Virginia Criminal Information Network (VCIN), a statewide network managed by the Virginia State Police. The VCIN is a gateway to several VSP systems including criminal history and wanted persons. VCIN also provides its users with a gateway to federal systems like the FBI's Interstate Identification Index (III) and National Crime Information Center (NCIC).

III contains criminal information about individuals, along with pointers to state systems where additional information may be available. NCIC contains, among other things, nationwide information about wanted persons and protective orders. Data from these systems are accessed through formatted messages rather than through direct database queries.

Access to VSP's SID based information and network infrastructure is important to achieving ICJIS program objectives. Naturally, the State Police are focused primarily on meeting the needs of the law enforcement community they serve. The ICJIS program is interested in leveraging agency information to improve business processes across all criminal justice agencies.

Architecturally, some level of integration between VCIN and ICJIS could provide benefits to both the VSP and the criminal justice community overall. For example:

- It will provide the State Police new ways to improve the quality of data stored on their systems, through improved inter-agency interfaces.

- It will allow ICJIS and the State Police to work cooperatively to cost effectively upgrade the statewide law enforcement computing infrastructure.
- It will allow ICJIS to improve the abilities of other agencies to positively identify and link data about offenders through access to the State Police's SID-based identification capabilities.

Integration of VCIN and ICJIS will not change the fact that the State Police will continue to own and manage the information stored in their databases. To the extent that ICJIS hardware and software facilitates the sharing and/or storage of information, ICJIS will be acting as a proxy for other criminal justice agencies. ICJIS is geared towards obtaining efficiencies that no single agency can accomplish on its own.

Given that there are both similarities and important differences in the mission of the Virginia State Police, as it relates to information systems, and ICJIS, there may be areas where the Virginia State Police and the ICJIS program can cooperate to achieve shared objectives. During the planning stages for ICJIS, consideration should be given to how the State Police and the ICJIS program can work together to meet shared objectives.

Among the issues to be resolved are potentially complex issues of security and data privacy affecting integration of VCIN and ICJIS. Security and privacy impact assessments will be conducted as part of any ICJIS/VCIN integration initiative.

6. Recommended Implementation Approach

Section Overview

Purpose: To describe a general plan for implementation of the ICJIS system.

Key Points:

- The ICJIS program is recommending a gradual approach to implementation, spread out in phases over several years, rather than a one-time "big bang" approach. Although the proposed architecture is not technologically complex, there is enough management complexity associated with planning and coordinating multiple agency integration activities to warrant a "one step at a time" approach.
- The ICJIS implementation plan is organized into a series of two-year phases, to reflect Virginia's biennial budgeting cycle.
- The current budget biennium (FY00-02) is designated Phase 1, the Foundation Phase, during which the program is laying the technical and programmatic groundwork for successful ICJIS implementation in the following phases. One of the critical activities of this phase is development of a detailed plan and budget for implementation, in time to support the next budgeting cycle.
- The ICJIS program proposes to implement an Initial Operating Capability 1 (IOC-1) during the next biennium (FY02-04), including implementation of a core infrastructure and integration of selected high priority agency systems and users.
- The ICJIS program proposes to complete implementation of an Initial Operating Capability (IOC-2) during the following biennium (FY04-06), completing the integration of all designated high priority agency systems and users.
- Additional systems and capabilities will be considered for integration in the out years beyond FY04-06, as resources permit, leading to achievement of a Full Operating Capability (FOC).

The ICJIS approach to implementation is based on the same fundamental premise as our approach to system architecture—the realization that we are not starting from scratch. The Virginia criminal justice community has built up a legacy of effective business processes and information systems that are woven into the day-to-day operations of the agencies and people they support.

To achieve the ICJIS vision cost effectively, it would be unnecessary, and unwise, to require wholesale replacement of all these existing processes and systems with something entirely new. Some fresh thinking and change is necessary, but the changes will build on what has already been accomplished, rather than uproot it.

The ICJIS Program's plan for implementing the target architecture envisions a gradual,

incremental approach rather than a "big bang." We are recommending this approach to reduce program management and system engineering risk, as well as to permit a realistic allocation of limited staff and funding resources.

We understand that any plan at this stage is subject to change, but a framework plan is necessary so that legislators and executive decision-makers have a context and a baseline they can agree upon. The plan described below therefore is high level and deliberately incorporates a great deal of flexibility. A more detailed work plan will be maintained as part of the ICJIS Project Management Plan.

6.1 Phased Implementation Plan

As a practical matter, the ICJIS implementation plan is organized into two-year phases to reflect the budgeting cycle of the Commonwealth of Virginia. The Virginia fiscal year begins on July 1 and ends on the following June 30. The Governor submits a biennial budget for the executive branch in December of odd-numbered years, to cover programs and operations for the two fiscal years beginning on July 1 of the following year. The General Assembly then acts on the Governor's budget during the winter session following the Governor's submittal.

As shown in Figure 6.1-1, the current two-year budget biennium began on July 1, 2000, and continues through June 30, 2002. The next major budget cycle will begin with the submittal of the Governor's proposed budget in December 2001, to cover the two fiscal years beginning on July 1, 2002.

The ICJIS program will implement in calendar year 2001 selected components of the ICJIS architecture as part of the ICJIS Charge Standardization Project. These components will focus on the sharing of charge information. The scope of this project is described in the business case for the Charge Standardization Project.

The ICJIS program is targeting the FY02-04 cycle to begin a more general implementation of the ICJIS architecture among the state ICJIS agencies. The objective at the end of this first implementation phase is to have the critical infrastructure in place, and to have selected high priority agency systems at least partially integrated, providing major benefits to the participating agencies. This initial level of integration is designated as Initial Operating Capability 1 (IOC-1).

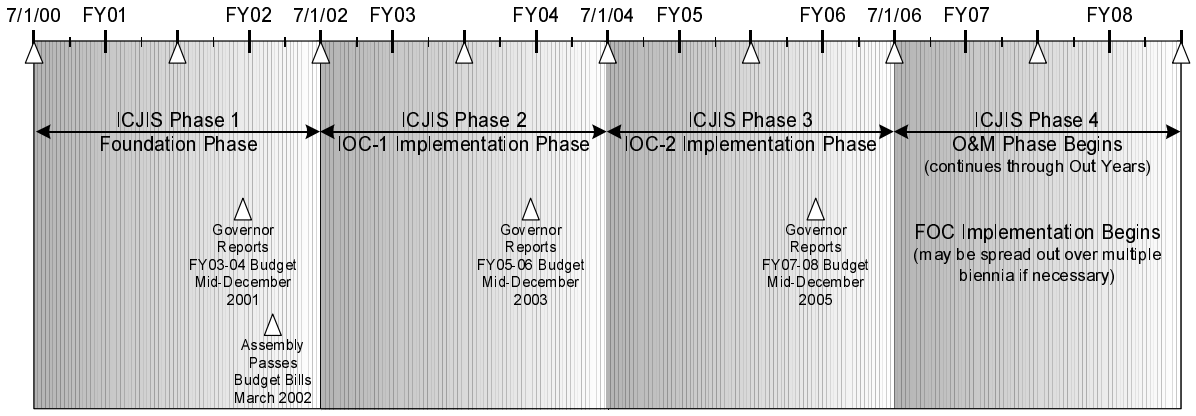

Figure 6.1-1. ICJIS Phases Based on Virginia's Two-Year Budgeting Cycle

To spread out funding requirements, as well as to manage risk, our plan is to complete implementation of the ICJIS architecture among the ICJIS agencies during the succeeding FY04-06 cycle. The objective at the end of this second implementation phase is to have all selected high-priority agency systems integrated, providing major benefits to the entire criminal justice community. This second level of integration is designated as IOC-2.

After IOC-2, the objective will be to implement a Full Operating Capability (FOC) by integrating additional systems, agencies, and functionality, as resources permit and as prioritized by the Steering Committee. We anticipate that this additional level of integration may also be scheduled incrementally over multiple budget biennia if necessary to spread resource requirements.

The current FY00-02 cycle is being devoted to laying all the necessary groundwork for a successful ICJIS implementation. This includes program planning and system engineering activities needed to support coordinated planning and consolidated budget estimates in time for the Governor's December 2001 budget submittal.

As illustrated in Figure 6.1-1, the current two-year budget cycle is designated as Phase 1. The subsequent two IOC implementation cycles are designated Phase 2 and Phase 3. Beyond Phase 3, in addition to FOC implementation, there will be a requirement to continue to maintain and periodically upgrade the ICJIS infrastructure. This currently open-ended period is designated Phase 4.

Besides spreading resource requirements over time, this multi-phase approach to ICJIS implementation reduces program management and system engineering risk. Although the technological solutions are largely available as commercial off-the-shelf (COTS) products and are therefore not regarded as high risk, the requirement to coordinate changes to multiple agency systems makes a one-step-at-a-time approach highly advisable.

DCJS will apply the principles of continuous process improvement to the management of the program. The beginning of each successive budgeting cycle will be used to take stock of the successes and lessons learned from prior cycles, and to make any mid-course corrections that may be indicated.

The following subsections identify, at a high level, the types of activities, by phase, needed to proceed from our current status to a viable realization of the ICJIS vision. At this level of discussion, activities are defined very generically. As part of Phase 1, DCJS will develop a work plan identifying activities at a greater level of detail. As each phase is executed, the work plan will be used to plan and monitor a logical, orderly progression of the detailed activities.

6.1.1 Phase 1: ICJIS Foundation Phase (FY00-02)

Fiscal Years 2001 and 2002 (July 1, 2000 through June 30, 2002) constitute Phase 1, during which the technical and programmatic groundwork is being laid to make ICJIS implementation possible in the following two phases. Activities include completion of detailed plans and requirements analyses, selection of technical and data standards, and design of a framework ICJIS system architecture.

Products of this phase will include:

- This detailed ICJIS Business Case document, which explains the objectives

and benefits of the program, and why it deserves the support of decision-makers and funding sources.

- A Project Management Plan, which describes the methodologies DCJS will use to plan and manage the system engineering and implementation activities required to implement the program.
- A Common Data Dictionary, which analyzes data items needed by multiple criminal justice agency systems, and establishes enterprise-wide standards so that data may be more easily shared.
- An ICJIS Computer System Assessment, which surveys the functions and technical characteristics of major Virginia criminal justice agency systems, to provide a baseline for identifying best technical approaches and estimating resources needed to support integration objectives.

Also during Phase 1, the ICJIS program has initiated a major subproject called the Charge Standardization Project (CSP). The CSP is aimed at laying a foundation for inter-agency integration by implementing the beginnings of an Integrated Magistrate System based on standardized Offense Tracking Numbers and Offense Codes.

An Integrated Magistrate System is a critical priority because, in Virginia's criminal justice system, local magistrate offices are typically where new charges are filed against suspected offenders. Basic information about charges and suspects are initially captured by local magistrates in the form of arrest warrants, which then become the basis for all subsequent case processing by the many other agencies in the state criminal justice community. At present, the lack of data standards and network interfaces between magistrate computer systems and other agency systems prevents the automated sharing of such data.

In Phase 1, the CSP will establish the prerequisite data standards and will implement the basic capabilities and interfaces of an Integrated Magistrate System, suitable for further development and statewide deployment in future phases. Further information on the CSP project may be found in the CSP Business Case document.

At the time of writing, DCJS has identified only partial funding needed to complete all desired Phase 1 activities. Should complete funding not be obtained in time, completion of some less critical activities may be deferred to Phase 2.

The highest strategic priority, from a program management standpoint, is to complete analyses, plans, and budgetary estimates needed to secure adequate and stable funding to proceed into Phase 2 and beyond. DCJS, with agency support, is developing consolidated resource requirements and budgetary estimates for implementation of ICJIS in phases 2 and 3, and for yearly operations and maintenance in the out-years. These estimates will be the basis for ICJIS budget submittals to the Governor beginning with the next (FY02-04) biennial budget cycle.

6.1.2 Phase 2: ICJIS IOC-1 Implementation (FY02-04)

Fiscal Years 2003 and 2004 (July 1, 2002 through June 30, 2004) constitute Phase 2, during which core ICJIS capabilities will be developed and integrated. At the end of this phase, a baseline infrastructure and key agency systems will have been integrated, and major benefits will have begun to be realized by the community of users. In some

cases, due to funding or logistical constraints, an agency system may be partially integrated during this phase, with complete integration delayed until Phase 3.

Defining exactly which systems will be integrated in Phase 2, and to what degree, is part of the ongoing planning process, and is dependent on the anticipated level of available funding. But in general terms, the ICJIS program plans to perform the following types of activities:

- Design and implement basic ICJIS infrastructure components, such as ICJIS user interfaces and central server capabilities
- Upgrade selected high-priority agency systems to implement ICJIS network interfaces
- Design and deploy basic implementations of the major SEARCH/ NASIRE integrating functions—query, push, pull, subscribe/notify, and publish—plus assemble
- Continue implementation and deployment of an Integrated Magistrate System under the Charge Standardization Project
- Operate and maintain ICJIS system components after deployment

At the appropriate time, based on accomplishments and lessons learned, DCJS and the agencies will coordinate updates to work plans and budget estimates for ICJIS integration activities in Phase 3. These updated plans and estimates will be the basis for ICJIS budget submittals to the Governor for the Phase 3 budget cycle.

6.1.3 Phase 3: ICJIS IOC-2 Implementation (FY04-06)

Fiscal Years 2005 and 2006 (July 1, 2004 through June 30, 2006) constitute Phase 3, during which the remaining high priority systems within the participating ICJIS agencies will be integrated into the ICJIS network. At the end of this phase, all major ICJIS integration functions will be operational, providing significant benefits to a full range of Virginia criminal justice agencies and users.

Defining exactly which systems will be integrated in Phase 3, and to what degree, is part of the ongoing planning process, and is dependent on anticipated levels of available funding. But in general terms, the ICJIS program plans to perform the following types of activities:

- Complete the implementation of major ICJIS infrastructure components, such as ICJIS user interfaces and central server capabilities
- Upgrade additional high-priority agency systems to implement ICJIS network interfaces
- Complete the implementation and deployment of the major SEARCH/ NASIRE integrating functions—query, push, pull, subscribe/notify, and publish—plus assemble
- Complete the implementation and deployment of an Integrated Magistrate System and related capabilities under the Charge Standardization Project
- Operate and maintain ICJIS system components after deployment

At the appropriate time, based on accomplishments and lessons learned, DCJS

and the agencies will coordinate work plans and budget estimates for further ICJIS integration activities in Phase 4. These plans and estimates will be the basis for ICJIS budget submittals to the Governor for the Phase 4 budget cycle.

6.1.4 Phase 4: ICJIS Maintenance and FOC Implementation (FY06-08 and Beyond)

Fiscal Years 2007 and 2008 (July 1, 2006 through June 30, 2008) mark the beginning of Phase 4, during which additional agencies and systems may be integrated into the ICJIS network. This phase is currently open-ended to leave flexibility for later definition of the ultimate ICJIS FOC configuration.

In general terms, the ICJIS program plans to perform the following types of activities:

- Upgrade additional agency systems to implement ICJIS network interfaces and integration functions
- Operate and maintain ICJIS system components after deployment
- Periodically evaluate emerging technologies for insertion into the ICJIS architecture
- Participate in national and international initiatives to improve criminal justice information sharing

As previously noted, Phase 4 activities may be spread over multiple budget biennia as necessary to spread resource requirements.

6.2 Program Organization and Responsibilities

To execute the multi-phase implementation plan and achieve the ICJIS vision, DCJS has organized a cost-effective team of experienced and dedicated program management professionals, guided by an inter-agency steering committee representing key stakeholder organizations. Figure 6.2-1 shows a first-level view of the ICJIS program organization.

The members of the Steering Committee—listed in Appendix A—represent the key Commonwealth agencies most immediately affected by the program. The Steering

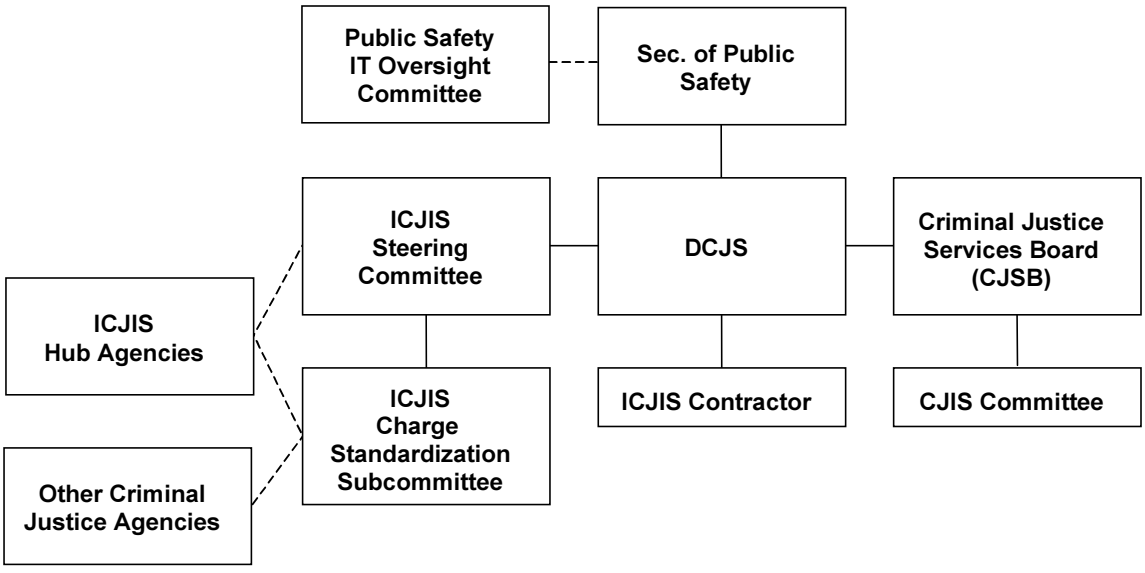

Figure 6.2-1. ICJIS Management Structure

Committee is the primary mechanism for inter-agency coordination on ICJIS issues. The Steering Committee meets monthly on a regularly scheduled basis, with additional working meetings held as needed.

A contract to provide system engineering and implementation support to ICJIS was awarded to Litton PRC on October 28, 1999. Through this contract, DCJS has access to a wide range of technical and management consulting expertise.

More detailed descriptions of the ICJIS organization, as well as project management plans and procedures, may be found in the Project Management Plan.

6.3 Plan for Coordinating Inter-Agency Developments

By its nature, the ICJIS program requires a high degree of continual coordination among DCJS and the participating agencies. In addition to coordination of ICJIS implementation activities, there is a requirement that future agency information system development activities be coordinated with ICJIS to ensure interoperability with related ICJIS systems and standards.

As discussed in the previous section, an ICJIS Steering Committee has been formed with representatives from key stakeholder agencies. The Steering Committee has been, and will continue to be, the primary mechanism for raising and resolving strategic inter-agency issues concerning the ICJIS program.

As the program initiates more detailed design and development activities, it is expected that lower-level working groups will be convened under the auspices of the Steering Committee. An example is the ICJIS Charge Standardization Project Advisory Committee, which is currently working on developing inter-agency standards related to management of offense and case information.

One mechanism for implementing subprojects involving other agencies will be through the administration of grants to the participating agencies. Requirements for each grant will be approved by the Steering Committee, and these requirements will become part of the grant application. Project reports described in the Project Management Plan will be used to monitor and control these projects.

Other administrative mechanisms to be used to coordinate and document inter-agency agreements will be Memoranda of Understanding (MOUs) and Memoranda of Agreement (MOAs). MOUs will be used to document general agreements on policies, plans, and technical designs. MOAs will be used to document agency commitments to specific actions and milestones. As the program manager for the overall ICJIS effort, DCJS will coordinate all MOUs and MOAs and will be a signatory to them.

A master project schedule will be maintained by DCJS and used to coordinate major inter-agency projects. DCJS will identify and monitor dependencies and critical paths among all agreed-upon agency and DCJS activities.

At a technical level, a critical coordinating mechanism will be the suite of standards agreed upon as applying to all ICJIS systems. To ensure interoperability, all systems on the ICJIS network will have to abide by agreed-upon architecture standards, network protocols and message formats, and common data dictionary standards, including shared unique IDs.

6.4 Resource and Budgetary Estimates

One of the critical objectives of the ongoing Phase 1 of the ICJIS program is to arrive at coordinated resource and budget estimates for ICJIS implementation activities in Phases 2 and 3. This objective must be met in time to support the Governor's next budget submittal in December 2001.

As was discussed in Section 6.1.1, many of the activities in Phase 1 are designed to support reliable cost estimation, as well as cost and risk reduction, in Phases 2 and 3. This specifically includes defining changes required on agency systems to link them into the ICJIS architecture, so that agencies can evaluate technical and resource impacts.

In order to give decision-makers a consolidated view of ICJIS budget requirements, DCJS will coordinate and consolidate ICJIS-related resource requirements and cost estimates as they are developed. DCJS will then submit a consolidated budget request through appropriate executive channels. Upon receipt of funds, DCJS will serve as a program management and grant-making agent, disbursing funds to itself and to participating agencies as needed to execute the agreed-upon implementation plan.

6.5 Measurement of Benefits

DCJS will evaluate and report the benefits realized from ICJIS implementation throughout the course of the program. Participating agencies will cooperate with DCJS to collect and report the necessary raw data from within their agencies.

Certain types of benefits are open to numerical and statistical reporting. Such categories might include cost reduction or avoidance, improved worker productivity, reduced case latency, increased case throughput, decreased information response time, data error reduction, etc. In such cases, DCJS will cooperate with participating agencies to collect the required raw data in an unobtrusive manner.

There are other types of benefits that are inherently subjective, intangible, or otherwise difficult to measure. Examples might include improved worker morale, improved public confidence, and improved public safety (e.g., by getting criminals off the street quicker). In some cases, subjective benefits could be numerically evaluated using techniques like periodic surveys. In other cases, evidence of benefits may have to be captured anecdotally.

7. Conclusion

After reviewing the previous sections, readers should recognize the following key points:

- The ICJIS is an important and timely program, offering mission-critical benefits to the Virginia criminal justice community, while supporting major IT standardization initiatives at state and federal levels.
- The underlying need for the ICJIS program is substantiated by a report on the Central Criminal Records Exchange, dated January 15, 2001 (http://www.apa.state.va.us/reports/special/searchreportname.asp), by the Auditor of Public Accounts. The report makes important recommendations regarding the need for more complete integration of criminal justice systems.
- The ICJIS program has a realistic technical approach and a realistic plan for realizing the ICJIS vision, as well as an effective organization in place to implement the plan.
- The ICJIS program is off to a good start and has initiated critical program planning and system engineering activities required to make ICJIS implementation feasible.

Having laid the programmatic groundwork, the ICJIS program now requires funding commitment and support to proceed with further planning and implementation activities.

7.1 Recommendations for Action

The ICJIS program recommends the following major decisions and actions by key players in the Virginia decision-making community:

- Discretionary state grant funding should be allocated and authorized to complete the planning and system engineering tasks begun in Phase 1 and listed in Section 6.1.1, during the next budget biennium.
- Agencies that may be potentially affected by ICJIS implementation should become (or remain) actively involved in ongoing planning and system engineering activities. It would be far more cost-effective to accommodate individual agency preferences and concerns early in the process rather than later.
- Executive, legislative, and judicial decision-makers should be planning to support ICJIS implementation funding requests in the next two budget biennia. Requests for additional information in advance of the budgeting process should be directed to the ICJIS program office.

The key to the success of any major multi-agency project is the committed support of decision-makers with the responsibility to promote strategic objectives. Given that commitment, and adequate resources to do the job, ICJIS promises to be an ultimate win-win for all parties involved.

7.2 Points of Contact

The ICJIS staff welcomes comments and questions concerning material in this Business Case. Please direct any inquiries to one of the following DCJS personnel:

Greg Lilley
Department of Criminal Justice Services
805 E. Broad Street, 10th Floor
Richmond, VA 23219

Phone: (804) 225-4863
Fax: (804) 786-9656
E-mail: glilley@dcjs.state.va.us

Ken Allen
Department of Criminal Justice Services
805 E. Broad Street, 10th Floor
Richmond, VA 23219

Phone: (804) 786-3973
Fax: (804) 786-9656
E-mail: kallen@dcjs.state.va.us

ICJIS Steering Committee

Name	Agency/Mailing Address	Phone Number/ Fax Number	E-mail
Mary Kaye Walker	Department of Motor Vehicles 2300 West Broad Street Richmond, VA 23220	(804) 367-8429	dmvmkw@dmv.state.va.us
Ben Lehman	Department of Information Technology 110 South Seventh Street Richmond, VA 23219	(804) 371-5573 (804) 786-4177	Blehman.dit@state.va.us
Barry Cross	Information Systems Technology Chesterfield County P. O. Box 40 Chesterfield, VA 23832	(804) 748-1563	CrossB@co.chesterfield.va.us
Bob Haugh	Department of Corrections 6900 Atmore Drive Richmond, VA 23261	(804) 674-3461 (804) 674-3495	haughwr@vadoc.state.va.us
Harry Heckel	Department of Juvenile Justice P. O. Box 1110 Richmond, VA 23218	(804) 786-3350	heckelhl@djj.state.va.us
Greg Lilley	Department Criminal Justice Services 805 East Broad Street, 10th Floor Richmond, VA 23219	(804) 225-4863 (804) 786-9656	glilley@dcjs.state.va.us
Ken Mittendorff	Supreme Court of Virginia 100 North Ninth Street Richmond, VA 23219	(804) 786-7816 (804) 786-4542	kmittendorff@courts.state.va.us
Naseem Reza	Virginia State Police 7700 Midlothian Turnpike Richmond, VA 23235	(804) 674-2202 (804) 674-2672	nreza@vsp.state.va.us
Anne Wilmoth	State Compensation Board 202 N. Ninth St., 10th Floor Richmond, VA 23219	(804) 786-0786 xt 222 (804) 371-0235	awilmoth@scb.state.va.us
Dan Ziomek	Department of Technology Planning 110 South 7th Street, Suite 135 Richmond, VA 23219	(804) 371-2763 (804) 371-2795	dziomek@dtp.state.va.us